Commissariat
à la protection de
la vie privée du Canada

Vie privée et réputation
Qui façonne votre identité en ligne?

Rapport annuel au Parlement 2012

Rapport concernant la *Loi sur la protection des renseignements personnels et les documents électroniques*

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario) K1A 1H3

Téléphone : 613-947-1698, 1-800-282-1376
Télécopieur : 613-947-6850
ATS : 613-992-9190

© Ministre des Travaux publics et des Services gouvernementaux Canada 2013

Image de couverture : Michael Rhodes, Paladin Design

N° de catalogue : IP51-1/2012F-PDF
1913-3375

Cette publication se trouve également sur notre site Web à **www.priv.gc.ca**

Suivez-nous sur Twitter : @privacyprivee

CHARGEMENT...

Vie privée et réputation

Qui façonne votre identité en ligne?

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Juin 2013

L'honorable Noel A. Kinsella, sénateur
Président
Sénat du Canada
Ottawa (Ontario) K1A 0A4

Monsieur,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* pour la période s'échelonnant du 1er janvier au 31 décembre 2012.

Je vous prie d'agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection
de la vie privée du Canada,

Original signé par

Jennifer Stoddart

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Juin 2013

L'honorable Andrew Scheer, député
Président
Chambre des communes
Ottawa (Ontario) K1A 0A6

Monsieur,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* pour la période s'échelonnant du 1er janvier au 31 décembre 2012.

Je vous prie d'agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection
de la vie privée du Canada,

Original signé par

Jennifer Stoddart

Table des matières

Message de la commissaire **1**

À propos du présent rapport **5**

La protection de la vie privée en chiffres en 2012 ..... **6**

Chapitre 1 – Pleins feux sur les citoyens : *Façonner votre réputation en ligne* **7**

1.1 Enquête d'une plainte : *Un faux compte Facebook est créé au nom d'une adolescente* 8

1.2 Enquête d'une plainte : *Les profils du site de rencontre PositiveSingles se retrouvent sur d'autres sites de rencontre* 12

1.3 Mise à jour d'une enquête : *Le nouveau propriétaire du site de réseautage social Nexopia s'engage à régler tous les problèmes liés à la protection de la vie privée* 18

1.4 Avancement des connaissances en matière de protection de la vie privée en ligne 20

Chapitre 2 – Pleins feux sur les entreprises : *Pourquoi la responsabilité vous revient* **23**

2.1 Lignes directrices en matière de responsabilité 24

2.2 Enquête sur une plainte déposée par la commissaire : *L'entreprise de location Aaron's utilise un logiciel espion pour retrouver des ordinateurs portatifs* 26

2.3 Enquête sur une plainte : *Un assureur utilise les cotes de crédit pour fixer les primes d'assurance, à l'insu des clients* 28

2.4 Enquête sur une plainte : *Une société de prêts hypothécaires recueille les renseignements personnels d'un couple à son insu et sans son consentement* 31

2.5 Enquête sur une plainte : *Une agente d'assurance communique des renseignements de nature délicate dans un message laissé sur une boîte vocale* 32

2.6 Enquête sur une plainte : *Un employé d'une banque commet une erreur en communiquant les données d'un homme à son épouse* 34

2.7 Enquête collaborative sur une plainte : *WhatsApp Messenger prend des mesures pour atténuer les risques d'atteinte à la vie privée dans son application mobile* 35

2.8 Enquête sur une plainte : *Une entreprise de télécommunications ne respecte pas ses propres politiques relatives aux demandes d'accès aux renseignements personnels* 39

2.9 Enquête sur une plainte : *Des camps d'été échangent des renseignements sur un enfant sans le consentement parental* 41

2.10 Enquête sur une plainte : *Un magasin cesse de capter, à l'aide d'une caméra, des images de la cour de son voisin* 43

2.11 Atteintes à la protection des données 44

2.11.1 *LinkedIn intervient promptement pour limiter les dommages à la suite d'une importante cyberattaque* 46

2.11.2 *Un employé d'une entreprise de services de placements répond à un courriel « hameçon »* 47

2.11.3 *Un ordinateur portatif est volé en même temps que des renseignements concernant le mot de passe* 47

2.12 Mise à jour de la politique de confidentialité de Google : *Des préoccupations demeurent en ce qui concerne le regroupement des données et leur conservation* 47

2.13 Mise à jour d'une vérification de conformité : *Une autorité indépendante confirme que Bureau en Gros a répondu aux préoccupations relatives à la protection de la vie privée* 48

Chapitre 3 – Pleins feux sur le Commissariat : *Répondre à vos préoccupations en matière de protection de la vie privée* **51**

3.1 Centre d'information 52

3.2 Réception des plaintes 53
3.2.1 Observations écrites reçues 53
3.2.2 Plaintes acceptées, par secteur d'activité 54
3.2.3 Types de plaintes acceptées 55
3.3 Règlement rapide des plaintes 56
3.3.1 *Une entreprise de services publics cesse de recueillir certains renseignements personnels* 57
3.3.2 *Un détaillant étranger remplace le NAS par un NIP* 57
3.3.3 *Une compagnie d'assurances supprime des dossiers archivés pour se conformer aux règles de conservation* 58
3.3.4 *Une entreprise propose à ses employés une nouvelle formation sur le traitement des demandes liées à la protection de la vie privée* 58
3.4 Servir la population canadienne au moyen d'enquêtes sur les plaintes 59
3.5 Avancement des connaissances 60
3.5.1 Programme des contributions 60
3.5.2 Recherche concernant les fuites sur Internet 63
3.5.3 Comprendre l'analyse prédictive 65
3.5.4 Tests génétiques offerts en ligne directement aux consommateurs 65
3.6 Établir un dialogue avec les entreprises 66
3.6.1 Le bureau de Toronto 67
3.6.2 Sondage auprès des entreprises 68
3.7 Lignes directrices, politiques et outils 69
3.7.1 Politique relative à la publicité comportementale en ligne 70
3.7.2 Document d'orientation sur l'infonuagique à l'intention des PME 71
3.7.3 Trousse d'urgence pour la protection des renseignements personnels 72

Chaptitre 4 – Pleins feux sur les institutions: *La LPRPDE et l'évolution du droit à la vie privée*..... 73
4.1 Au Parlement 75
4.1.1 *La commissaire témoigne lors des audiences sur la vie privée et les médias sociaux* 76
4.2 Devant les tribunaux 77
4.2.1 *Commissaire à la protection de la vie privée c. Association of American Medical Colleges* 77
4.2.2 *X c. Banque Toronto-Dominion et al* 79
4.2.3 Demandes de contrôle judiciaire : *X c. commissaire à la protection de la vie privée du Canada* 80
4.2.4 Demande de contrôle judiciaire : *X c. procureur général du Canada et commissaire à la protection de la vie privée du Canada* 80
4.2.5 Intervention devant la Cour suprême du Canada : *X c. Bragg Communications Inc.* 80
4.3 Lois provinciales et territoriales essentiellement similaires 82
4.4 Collaboration avec les homologues provinciaux et territoriaux 83
4.5 Initiatives mondiales 84
4.5.1 Application concertée 85
4.5.2 Autres activités internationales 86

Table des matières

L'année à venir **89**

Annexe 1 — Définitions **93**
Définitions des types de plaintes déposées en vertu de la LPRPDE 93
Définitions des conclusions et autres décisions 94
Processus d'enquête 96

Annexe 2 — Statistiques sur les enquêtes liées à la LPRPDE pour 2012 ..... **98**
Plaintes acceptées par secteur d'activité 98
Plaintes acceptées par type de plainte 100
Plaintes fermées par secteur d'activité et décision 101
Plaintes fermées par type de plainte et décision 102
Délais de traitement moyens par décision 103
Délais de traitement moyens par type de plainte et de règlement 104
Signalements volontaires des atteintes à la protection des données par secteur d'activité et type d'incident 105

À propos de la LPRPDE

La *Loi sur la protection des renseignements personnels et les documents électroniques*, ou LPRPDE, établit des règles de base à l'égard de la gestion des renseignements personnels dans le secteur privé.

Elle vise l'atteinte d'un juste équilibre entre le droit à la protection des renseignements personnels des individus et le besoin qu'ont les organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins commerciales légitimes.

La LPRPDE s'applique aux organisations qui se livrent à des activités commerciales partout au pays, sauf dans les provinces qui disposent d'une loi essentiellement similaire sur la protection des renseignements personnels applicable au secteur privé. Le Québec, l'Alberta et la Colombie-Britannique disposent d'une telle loi. Toutefois, même dans ces provinces, la LPRPDE s'applique aux entreprises du secteur privé sous réglementation fédérale ainsi qu'aux renseignements personnels obtenus dans le cadre de transactions interprovinciales et internationales.

La LPRPDE protège également les renseignements des employés travaillant dans les secteurs sous réglementation fédérale.

Message de la commissaire

Presque treize ans après l'adoption de la *Loi sur la protection des renseignements personnels et les documents électroniques*, il semble indiqué d'examiner l'évolution spectaculaire du contexte dans lequel la loi s'inscrit.

Lorsque la loi qui fait l'objet du présent rapport a été adoptée en 2000, l'« hameçonnage » se faisait sur les lacs, le diminutif « appli » n'évoquait rien de spécial et nos « amis » étaient des gens qu'on connaissait. Les achats en ligne constituaient une nouveauté et les services bancaires sur Internet en étaient au stade embryonnaire. Dans les salles d'attente et aux arrêts d'autobus, les gens se tournaient les pouces; ils ne les faisaient pas s'agiter sur de petits écrans.

Malgré toutes les merveilles et les commodités de l'ère du numérique, des éléments indésirables sont présents. Pensons, par exemple, aux fraudes et aux escroqueries en ligne, aux atteintes à la protection des données qui prennent parfois des proportions colossales, à la capacité d'explorer la vie des autres de façon secrète, voire malicieuse, à la cyberintimidation et à la possibilité de ruiner des réputations facilement et sous le couvert de l'anonymat.

Cette évolution frénétique fait que la protection de la vie privée n'est pas un jeu d'enfant. Elle nécessite une loi stricte et mûre, nuancée et efficace. La LPRPDE, qui a été conçue au siècle dernier, n'est plus à la hauteur de la tâche.

Bien sûr, nous avons obtenu de bons résultats au cours des douze premières années. Nos enquêtes et vérifications visant des titans d'Internet comme Facebook et Google, des géants de la distribution comme Winners et Bureau en Gros, de grandes entreprises comme Air Canada et la CIBC, ainsi que des centaines d'organisations plus petites, ont aidé à forger et à promouvoir le droit à la vie privée des Canadiennes et Canadiens.

À quoi pouvons-nous attribuer ces bons résultats? Je dois ici rendre hommage aux citoyennes et aux citoyens canadiens qui ont pris le temps de nous faire part de leurs inquiétudes en matière de protection de la vie privée, à notre équipe qui n'a pas ménagé ses

efforts pour répondre à leurs préoccupations, ainsi qu'au monde des affaires. La plupart des entreprises qui brassent des affaires au Canada comprennent la valeur de la protection de la vie privée et reconnaissant son importance pour les clients. Il est gratifiant de constater les progrès que nous avons accomplis pour ce qui est de clarifier les notions de consentement, de responsabilité et de transparence, ainsi que les autres principes relatifs à l'équité dans le traitement de l'information qui sont inscrits dans la LPRPDE aujourd'hui.

Toutefois, il est aussi très décourageant de voir que d'importantes organisations canadiennes font systématiquement preuve de négligence dans la protection de la vie privée, comme le montrent nos études de cas.

Dans d'autres organisations, il est malheureusement évident que la résolution des problèmes exige un investissement considérable, voire total, en ressources et en temps.

Comme cela est clairement formulé dans le présent rapport, nous avons peut-être fait tout ce qui était en notre pouvoir avec la loi en vigueur, qui a peu évolué depuis le jour de son adoption.

Enjeux nouveaux

La réalité d'aujourd'hui est que la vie en ligne, les nouvelles technologies de forage de données, le désir des autorités chargées de l'application de la loi de disposer de preuves numériques, la multitude des nouvelles cybermenaces et les modèles commerciaux contemporains fondés sur l'infonuagique exigent que nous abordions d'une façon très différente la protection des renseignements personnels.

Il s'agit d'enjeux mondiaux qui nécessitent des solutions mondiales. Nous devons collaborer avec nos homologues internationaux, mais l'action collective fonctionne le mieux lorsque toutes les administrations disposent d'instruments comparables.

Aujourd'hui, avec la LPRPDE, nous n'avons plus un instrument comparable à celui des autres pays; notre retard est trop grand. Dans les autres pays, les autorités de protection des données ont le pouvoir légal de rendre des ordonnances exécutoires, d'imposer des amendes lourdes et de prendre des mesures significatives dans le cas d'atteintes importantes à la protection des données; quant à nous, nous devons utiliser une méthode « douce » : persuasion, encouragements et, au pire, possibilité de publier les noms des transgresseurs dans l'intérêt public. Dans de nombreux cas, le résultat de notre travail est que les entreprises adoptent des pratiques plus respectueuses de la vie privée, mais le coût est généralement très élevé pour ce qui est du temps et des ressources. Et, poussés dans nos derniers retranchements, à défaut de livrer une bataille juridique coûteuse et chronophage, nous n'avons pas le pouvoir de faire appliquer nos recommandations. L'ajout de mesures d'application de la loi plus vigoureuses à la LPRPDE inciterait les organisations à prendre leurs responsabilités plus au sérieux et à mettre en place des mesures de protection de la vie privée dès le départ, en sachant que les conséquences sur le plan financier d'une atteinte en vertu d'un régime plus strict pourraient être réelles et importantes.

La LPRPDE se trouve aujourd'hui à un point tournant de son histoire. Il faut maintenant l'obliger à se lever du canapé et à assumer des responsabilités plus grandes, comme on le ferait pour un jeune qui s'apprête à célébrer son treizième anniversaire.

***

Je me trouve aussi à la croisée des chemins : mon mandat se termine dans quelques mois seulement. Après dix années comme commissaire à la protection de la vie privée, je présente devant le Parlement mon dernier rapport annuel concernant la LPRPDE.

Quand je fais le bilan de ces dix années, j'éprouve un sentiment de fierté pour ce que nous avons accompli et les gens talentueux que nous avons attirés. J'ai eu la chance extraordinaire d'être entourée d'un personnel accompli dans les domaines de la réalisation d'enquêtes, de la vérification de la conformité, de l'élaboration des politiques, de la technologie, de la recherche, de la sensibilisation du public et de la loi, et qui a vraiment à cœur de protéger le droit à la vie privée des Canadiennes et Canadiens.

Je me réjouis également des changements que j'ai observés dans les organisations canadiennes et chez nos concitoyens.

Notre plus récent sondage d'opinion suggère que les Canadiennes et Canadiens ont de plus en plus conscience du caractère sacré de leurs renseignements personnels. La plupart des personnes reconnaissent maintenant les risques que peuvent entraîner la publication en ligne de leurs coordonnées ou d'informations sur leurs allées et venues, ou la communication de leurs renseignements personnels à des sites Web qui leur semblent douteux.

Responsabilités multiples

D'autant plus réjouissant est le fait que les gens semblent comprendre qu'ils jouent un rôle primordial dans la protection de leurs renseignements personnels et de leur identité en ligne. En effet, notre sondage, effectué vers la fin de l'année 2012, a révélé qu'une majorité substantielle de gens avait décidé de ne pas installer une application, ou en avait désinstallé une, parce qu'elle exigeait la communication d'un trop grand nombre de renseignements personnels.

Le Commissariat a travaillé fort pour renforcer de tels messages dans l'esprit de la population. En pareil contexte, un thème clé exploré dans le présent rapport annuel a trait à l'identité au sein de l'univers en ligne et, plus particulièrement, à l'importance de contrôler sa propre réputation dans les médias sociaux. Vous y trouverez notamment des références à certains documents d'information à l'intention des particuliers que nous avons rendus publics l'année dernière, ainsi qu'un résumé des enquêtes que nous avons menées sur Facebook, Nexopia, réseau social s'adressant aux jeunes, et PositiveSingles, réseau de rencontre pour les personnes atteintes d'une infection transmissible sexuellement.

Cependant, les gens ne peuvent assumer la responsabilité de leurs activités en ligne que si les entreprises le leur permettent. Voilà pourquoi nos activités de sensibilisation, notre travail

auprès des tribunaux, nos efforts internationaux et nos actions au fil des ans ont eu pour but de persuader les entreprises qu'elles doivent mettre en place des programmes de gestion de la protection de la vie privée dignes de ce nom, des politiques compréhensibles sur le traitement des renseignements personnels et des pratiques efficaces de protection des données à tous les niveaux.

En vertu de la LPRPDE, les entreprises sont responsables des renseignements personnels qu'elles recueillent. Il s'agit d'un second thème clé exploré dans le présent rapport. Vous prendrez connaissance, dans les pages qui suivent, de nos nouvelles lignes directrices en matière de responsabilité et des orientations que nous avons fournies sur un vaste éventail de technologies et de pratiques commerciales; vous découvrirez également les mesures prises par LinkedIn pour réparer les dégâts provoqués par une importante fuite de données, ainsi qu'une enquête internationale innovatrice sur le service de messagerie WhatsApp.

Si les particuliers et les organisations sont prêts à jouer leur rôle respectif dans la protection de la vie privée, le gouvernement doit soutenir leurs efforts. Il ne fait aucun doute dans mon esprit que les enjeux en matière de protection de la vie privée continueront de prendre de l'ampleur et que, tôt ou tard, ils rendront impuissante la loi en vigueur.

Ainsi, à l'heure de quitter mon poste de commissaire à la protection de la vie privée, je ne peux qu'espérer que mon successeur assistera à la revitalisation de la LPRPDE dans l'intérêt des entreprises présentes au Canada et de l'ensemble des Canadiennes et Canadiens.

La commissaire à la protection de la vie privée du Canada,

Jennifer Stoddart

À propos du présent rapport

Comme le tableau *La protection de la vie privée en chiffres* l'atteste, 2012 a été une autre année bien remplie pour le Commissariat à la protection de la vie privée du Canada. Le présent rapport annuel donne des détails sur ces chiffres et présente de nombreuses autres activités que nous avons réalisées pour le compte du Parlement, des parties intéressées et de la population canadienne.

Tout au long de l'année, nous sommes restés fidèles à notre mission qui consiste à aider les Canadiennes et Canadiens à mieux assurer le respect de leur vie privée et la protection de leurs renseignements personnels. Pour ce faire, nous avons agi de différentes façons, comme en fait foi le découpage en chapitres du présent rapport.

Le **chapitre 1 : *Pleins feux sur les citoyens*** souligne un thème clé qui est ressorti de notre travail d'enquête et de nos autres activités en 2012. Intitulé « Façonner votre réputation en ligne », le chapitre décrit les menaces à l'identité et à la réputation des personnes que dissimule le cyberespace, et ce que le Commissariat a fait pour aider les Canadiennes et Canadiens à les reconnaître et à les atténuer.

Le **chapitre 2 : *Pleins feux sur les entreprises*** développe l'idée que les entreprises sont responsables des renseignements personnels sur les consommateurs qu'elles recueillent, utilisent, conservent et communiquent. Intitulé : « Pourquoi la responsabilité vous revient… », le chapitre illustre cette réalité au moyen de résumés de plaintes clés que nous avons examinées en 2012, ainsi que de fuites de données importantes qui nous ont été signalées. Le chapitre présente aussi les orientations que nous avons publiées au sujet de la responsabilité.

Le **chapitre 3 : *Pleins feux sur le Commissariat*** est intitulé « Répondre à vos préoccupations en matière de protection de la vie privée » parce qu'il fait état des préoccupations qui ont incité les Canadiennes et Canadiens à appeler notre Centre d'information ou à déposer une plainte auprès du Commissariat. Le chapitre résume le travail que nous avons fait pour répondre à ces préoccupations et témoigne de notre volonté constante de résoudre les problèmes en temps utile et d'une manière efficace. Il présente aussi les études en matière de protection de la vie privée que nous finançons ou que nous réalisons à l'interne, et il démontre comment la recherche nous aide à définir les orientations que nous fournissons aux organisations, à élaborer les produits d'information destinés aux particuliers et à nous acquitter de nombreux autres aspects de notre travail.

Enfin, le **chapitre 4 : *Pleins feux sur les institutions*** met l'accent sur nos efforts en vue de renforcer la loi sur la protection de la vie privée applicable au secteur privé du Canada. Intitulé « La LPRPDE et l'évolution du droit à la vie privée », le chapitre fait état des actions que nous avons menées auprès du Parlement et des tribunaux, ainsi que du travail que nous réalisons de concert avec les autorités provinciales, territoriales et internationales chargées de la protection de la vie privée, ainsi qu'avec d'autres organisations mondiales, pour le renforcement de la protection de la vie privée des Canadiennes et Canadiens.

La protection de la vie privée en chiffres en 2012

Demandes de renseignements et plaintes liées à la LPRPDE		
Demandes de renseignements reçues		4 474
Plaintes acceptées en vue de l'ouverture d'une enquête officielle		220
Enquêtes officielles achevées		
Enquêtes achevées avec conclusions satisfaisantes	140	145
Enquêtes considérées comme fondées et non réglées	5	
Plaintes acceptées en vue d'un règlement rapide		138
Plaintes acceptées en vue d'un règlement rapide qui ont été fermées		115
Plaintes acceptées en vue d'un règlement rapide transférées pour l'ouverture d'une enquête officielle		23
Avis d'incident liés à la LPRPDE		
Communication accidentelle	9	33
Perte	3	
Vol et accès non autorisé	21	
Affaires parlementaires*		
Lois ou projets de loi examinés sous l'angle de leurs répercussions sur la vie privée		14
Comparutions devant des comités parlementaires		10
Mémoires officiels rédigés		3
Autres rencontres avec des parlementaires ou leur personnel (par exemple, correspondance avec des députés ou des sénateurs)		57
Relations avec les parties intéressées et le public*		
Allocutions et présentations		101
Outils, politiques et documents d'orientation rendus publics		7
Accords de contribution signés		11
Consultations du site Web principal du Commissariat	1 950 086	2 923 759
Consultations des blogues et autres sites Web du Commissariat (dont le blogue du CPVP, le blogue des jeunes, le site Web des jeunes, le site de l'inspection approfondie des paquets et la chaine YouTube)	973 673	
« Gazouillis » envoyés		1 012
Abonnés Twitter au 31 décembre 2012		5 130
Publications distribuées		18 186
Communiqués et annonces		29

* Remarque : Sauf indication contraire, les données ci-dessus comprennent également les activités menées en vertu de la *Loi sur la protection des renseignements personnels*, qui sont décrites dans un rapport annuel distinct.

Façonner votre réputation en ligne

Nous sommes nombreux à beaucoup réfléchir à qui nous sommes et à la manière dont nous voulons être perçus.

Enfants, nous mettons des robes de princesse ou des costumes de super héros. En préparation de notre premier rendez-vous galant, nous implorons le miroir de nous déclarer charmant, « sexy » ou « cool ». Plus tard, dans le monde adulte, nous soignons méthodiquement notre apparence et nous projetons une image de notre choix, par exemple menuisier habile, infirmière attentionnée, agent immobilier averti ou commerçant fiable.

Cependant, dans l'univers en ligne, l'image et l'identité sont plus fluides et fragiles. Dans un monde où les mots n'engagent pas à grand-chose et où les images peuvent être publiées avec bienveillance ou désir de nuire, une réputation peut être redorée et noircie tout aussi facilement.

À chacun de juger, selon ses goûts et sentiments personnels, si la chose est bonne ou mauvaise. Toutefois, pour nous qui œuvrons dans le domaine de la protection de la vie privée, la maîtrise de la situation par les personnes est sûrement l'enjeu fondamental.

Nous estimons que les individus ont le droit de façonner leur réputation et d'être ce qu'ils veulent être en ligne. Il est toutefois essentiel que les sites Web soient transparents au sujet de leurs activités; ainsi, les personnes qui les utilisent pourront comprendre, prendre des décisions et exprimer leur consentement pour ce qui est du traitement de leurs renseignements personnels.

Dans le présent chapitre

Or, comme le révèle le présent chapitre, les choses ne sont pas toujours ce qu'elles devraient être. Prenons l'exemple du profil Facebook qui n'appartient pas à la personne représentée sur la photo; il s'agit d'un faux profil publié malicieusement par un imposteur.

Prenons aussi l'exemple du site de rencontre pour les personnes atteintes d'une infection transmissible

sexuellement dont la base de données s'avère être une « boîte de verre » : les membres y déposent leurs renseignements personnels et ceux-ci sont visibles sur une douzaine d'autres sites de rencontre faisant partie, sans que cela soit du tout apparent, du même réseau.

Le chapitre explore aussi des questions d'actualité comme la protection de la vie privée des jeunes et décrit des études que nous avons commandées ou financées pour mieux comprendre la gestion de la réputation dans le cyberespace.

1.1 ENQUÊTE D'UNE PLAINTE : *Un faux compte Facebook est créé au nom d'une adolescente*

Contexte

En 2012, nous avons enquêté sur une affaire dans laquelle une personne s'est fait passer pour une jeune adolescente sur Facebook. La jeune fille, âgée de 13 ans, n'avait jamais eu de compte Facebook, mais une personne en a créé un à son nom.

Le faux compte avait l'air bien réel. Il comprenait une photo de la jeune fille et invitait certains de ses amis du monde réel à se connecter, ou à devenir son « ami », comme il est d'usage de dire sur Facebook. L'imposteur a communiqué avec les nouveaux « amis », leur adressant des remarques déplacées qui semblaient provenir de la jeune fille.

Dès que l'adolescente a découvert qu'une personne se faisait passer pour elle sur le réseau social, sa mère a communiqué avec Facebook par courriel et a exigé que l'entreprise supprime immédiatement et définitivement le faux compte, ainsi que les messages qui en émanaient. Elle a aussi exigé que l'entreprise communique avec les prétendus « amis » du faux profil pour les informer de la tromperie.

La mère a aussi déposé une plainte auprès du Commissariat, en alléguant que Facebook Inc. avait enfreint sa propre Déclaration des droits et responsabilités en laissant un imposteur créer un compte Facebook au nom de sa fille.

Constatations

Notre enquête a permis d'établir que Facebook a mis en place un processus de signalement des faux comptes et que ce processus est décrit dans son aide en ligne. Il n'est pas nécessaire d'avoir un compte Facebook pour utiliser ce processus.

Une fois qu'il est avéré qu'un compte est faux, il peut être désactivé; toutes les contributions et tous les messages envoyés à partir du compte sont immédiatement supprimés du réseau social.

L'entreprise a confirmé au Commissariat qu'elle avait invoqué ce processus pour supprimer de façon permanente le faux profil et son contenu, y compris les messages qui en émanaient.

Elle a aussi déclaré que, moins de cinq jours après avoir déterminé que le compte était faux, elle avait

supprimé de ses systèmes les données personnelles fournies par la plaignante, conformément à la politique de Facebook qui prévoit la suppression ou la destruction des renseignements personnels qui ne sont plus nécessaires pour les motifs de leur collecte. La mère avait fourni la photo du passeport de sa fille et d'autres documents d'identité pour que Facebook puisse confirmer que le compte était faux.

Cependant, pour ce qui a trait à l'autre attente de la plaignante, à savoir que Facebook informe les « amis » du faux profil de la tromperie, l'entreprise nous a informés qu'elle n'envoyait pas d'avis du genre au nom des utilisateurs, conformément à sa politique générale, et qu'elle ne l'avait pas fait non plus dans l'affaire en question.

Selon Facebook, il ne serait ni indiqué, ni pratique, d'aviser les « amis » liés à un compte créé par un imposteur. L'entreprise a déclaré qu'elle proposait une plateforme, et qu'elle était ainsi une tierce partie dans les interactions en ligne. Les renseignements personnels, qu'ils soient exacts ou faux, sont communiqués par les personnes, et non pas par Facebook.

Concrètement, Facebook a aussi déclaré que, une fois qu'un compte est désactivé, toutes les contributions et tous les messages envoyés à partir du compte sont supprimés immédiatement. Si un imposteur ou un autre membre malveillant envoie des messages à d'autres utilisateurs de Facebook, ces messages disparaissent du système dès que le compte est désactivé.

Par ailleurs, l'entreprise a estimé qu'elle ne pouvait pas toujours déterminer quels problèmes signalés par les utilisateurs étaient légitimes. En cas de demande de désactivation d'un compte, Facebook peut vérifier l'identité du demandeur et donner suite à la demande si elle n'est pas contestée. Cependant, même dans ce cas, l'entreprise a déclaré qu'elle n'était pas en mesure d'affirmer avec certitude qu'un compte a été désactivé pour usurpation d'identité.

Pour cette raison, Facebook a estimé qu'il était préférable de laisser les individus eux mêmes agir contre les imposteurs de la manière qui leur paraissait la plus appropriée.

L'entreprise a aussi fait valoir que si elle commençait à aviser les « amis » d'un compte créé par un imposteur, l'intervention elle-même pourrait engendrer une escalade ou aggraver la situation, et même nuire encore plus à la personne dont l'identité a été usurpée.

En vertu de la LPRPDE, nous avons conclu que rien n'obligeait l'entreprise elle-même à aviser les personnes devenues « amies » d'un compte créé par un imposteur, parce qu'elle devrait alors intervenir dans des relations interpersonnelles et démêler le vrai du faux.

Autres préoccupations

Cependant, même si Facebook n'est pas tenu, en vertu de la LPRPDE, d'aviser les « amis » liés à un compte créé par un imposteur, nous continuons de nous préoccuper énormément des conséquences sur le plan de la réputation et des émotions que les victimes d'usurpation d'identité peuvent subir sur les réseaux sociaux.

Nous convenons que les utilisateurs de Facebook peuvent se servir de la plateforme pour corriger les renseignements erronés les concernant sur leur propre compte, et rétablir leur réputation avec leurs propres mots et selon leurs propres conditions. Nous demeurons toutefois inquiets pour les gens qui ne sont pas sur Facebook et, qui, de ce fait, n'ont pas la possibilité de savoir qui sont les « amis » trompés ou de communiquer avec eux pour dissiper toute confusion.

Nous avons donc insisté sur le besoin pour Facebook, en particulier dans les situations où des non-utilisateurs sont concernés, d'être plus responsable par rapport à son modèle d'activité, qui permet la création de comptes par des imposteurs en premier lieu. Nous encourageons l'entreprise à réparer ou à atténuer les préjudices sur le plan des émotions et de la réputation qui résultent de tels cas de violation du droit à la vie privée.

Après huit mois de consultation avec le Commissariat, l'entreprise a fini par accepter de mettre en œuvre un nouveau processus en vertu duquel elle examinera et vérifiera, au cas par cas, les cas d'usurpation présumée de l'identité de non-utilisateurs qui lui sont signalés, ainsi que les demandes d'aide des victimes apparentes.

Même si l'entreprise ne communiquera pas elle-même avec les « amis » d'un compte créé par un imposteur pour les informer d'une tromperie, elle a proposé de mettre en place un processus qui permettra aux non-utilisateurs d'informer eux-mêmes les « amis » en question pour restaurer leur réputation en ligne. Nous avons estimé que cette mesure donnera aux non-utilisateurs les mêmes moyens que ceux dont disposent les utilisateurs.

Cependant, dans l'affaire qui nous intéresse, le faux compte et les renseignements qu'il contenait ont été promptement supprimés; Facebook n'a donc pas pu proposer la nouvelle forme d'aide.

Nous avons conclu que Facebook avait fait preuve de diligence en désactivant et en supprimant rapidement le compte créé par un imposteur.

En guise de conclusion

Dans le cyberespace, les informations sont particulièrement omniprésentes et accessibles. En règle générale, elles sont aussi persistantes; seuls les efforts les plus énergiques permettent de les purger ou de les maîtriser. Lorsque ces informations sont dommageables ou erronées, elles peuvent menacer grandement la vie privée et la réputation d'une personne, en ligne comme dans le monde réel.

Étant donné la magnitude du risque, il est de la responsabilité de chacun, qu'il s'agisse des autorités de protection des données, des organisations ou des individus, de protéger les renseignements personnels en ligne.

L'affaire souligne l'importance de sensibiliser les jeunes et leurs parents aux risques liés à un mauvais usage de la technologie Internet. Elle nous rappelle d'être vigilants pour ce qui a trait aux renseignements en ligne nous concernant, et d'agir rapidement si ces renseignements sont faux, trompeurs ou

dommageables. Plus les renseignements erronés restent longtemps en ligne, plus ils risquent de porter atteinte à la réputation d'une personne.

Ces conclusions ont été renforcées lorsque le Commissariat a été autorisé à intervenir dans une autre affaire de cyberintimidation portée à l'attention de la Cour suprême du Canada en 2012.

Une victime de 15 ans s'est retrouvée impliquée dans l'affaire, qui a soulevé un éventail de questions qui sont des priorités stratégiques pour le Commissariat, notamment l'intégrité de l'identité, la protection de la vie privée des jeunes, les risques en matière de respect de la vie privée associés aux réseaux sociaux, ainsi que la nécessité d'établir des normes sociales et des règles de droit adaptées à l'ère d'Internet.

Comme nous l'expliquons plus en détail au chapitre 4, nous avons présenté, de vive voix et par écrit, des arguments qui précisent le cadre juridique que les tribunaux devraient retenir lorsqu'ils soupèsent le droit au respect de la vie privée par rapport au principe de la publicité des débats judiciaires.

Nouvelles ressources en matière de protection de la vie privée pour les jeunes

En 2012, nous avons continué de mettre au point de nouvelles ressources pour aider les enfants et les jeunes à relever les défis posés par la protection de la vie privée en ligne.

En particulier, nous avons dévoilé une trousse de présentations destinée aux élèves de la 4e à la 6e année, qui complètent la trousse que nous avions déjà distribuée pour les élèves de la 7e et de la 8e année (secondaire I et II au Québec) et de la 9e à la 12e année (secondaire III à V au Québec). Ces trousses aident les parents, les enseignants et les dirigeants locaux à proposer des présentations intéressantes et efficaces aux jeunes sur l'impact de la technologie sur la vie privée, ainsi que sur les compétences dont ils ont besoin pour protéger leur identité en ligne.

Nous avons aussi publié une bande dessinée romanesque intitulée *Branchés et futés : Internet et vie privée*, qui explique comment reconnaître et maîtriser les risques en matière de protection de la vie privée associés aux réseaux sociaux, aux appareils mobiles, aux textos et aux jeux en ligne.

Branchés et futés : Internet et vie privée (http://www.priv.gc.ca/youth-jeunes/index_f.asp)

De plus, nous avons organisé notre quatrième concours annuel de vidéos, intitulé *Ma vie privée et moi*, auquel participent des étudiants de partout au Canada.

Nos efforts visant à promouvoir la distribution de nos ressources destinées aux jeunes en matière de protection de la vie privée ont été bien reçus et ont attiré l'attention plus qu'auparavant. Des articles présentant notre bande dessinée romanesque, nos trousses de présentations et notre page Web « Vie privée des jeunes » sont parus dans des publications pour enseignants en Ontario et au Nouveau-Brunswick, dans *School Libraries in Canada* (SLIC), revue de la Canadian Association for School Libraries, ainsi que dans le *Canadian Teacher Magazine*.

À la fin de l'année, nous avions reçu plus de 170 demandes pour des exemplaires de notre bande dessinée romanesque de chaque province et territoire du Canada.

1.2 ENQUÊTE D'UNE PLAINTE : *Les profils du site de rencontre PositiveSingles se retrouvent sur d'autres sites de rencontre*

Contexte

PositiveSingles.com est un site de rencontre en ligne pour les personnes atteintes d'une infection transmissible sexuellement. Nous avons reçu une plainte de plusieurs personnes alléguant que PositiveSingles aurait communiqué leurs renseignements personnels à leur insu et sans leur consentement.

Les plaignants ont déclaré que, en établissant leurs profils en ligne, ils avaient communiqué des renseignements personnels confidentiels. Ils ont affirmé l'avoir fait sans crainte parce qu'ils croyaient que les renseignements seraient protégés. Leur conviction a été renforcée par un énoncé apparaissant sur la page d'accueil du site de PositiveSingles selon lequel l'entreprise s'engageait à ne pas « communiquer, vendre ou louer tout renseignement permettant d'identifier une personne à une tierce partie » [traduction].

Cependant, après avoir adhéré à PositiveSingles, les plaignants ont découvert que les photos de leur profil et des renseignements personnels très confidentiels, y compris des renseignements médicaux, qu'ils avaient fournis à PositiveSingles avaient commencé à apparaître sur de nombreux autres sites de rencontre. Plusieurs de ces sites Web ciblaient des personnes ayant des centres d'intérêt variés, présentant des caractéristiques démographiques différentes et dont les problèmes de santé étaient souvent complètement différents.

Par exemple, une plaignante nous a montré que son profil personnel était apparu sur 57 autres sites de réseautage social. Certains de ces sites étaient expressément conçus pour attirer des personnes ayant des préférences sexuelles particulières ou atteintes d'affections transmissibles, ou des personnes cherchant des rapports sexuels occasionnels, descripteurs qui ne correspondaient pas du tout, selon elle, au profil qu'elle avait publié sur PositiveSingles.

Les plaignants prétendaient que PositiveSingles ne les avait pas informés que les autres sites existaient, n'avait pas obtenu leur consentement pour la communication de leurs renseignements personnels à d'autres sites et ne leur avait proposé aucune option de non-participation.

De plus, les plaignants ont soutenu que, lorsqu'ils ont découvert que leurs renseignements personnels avaient été communiqués à d'autres sites, ils ont demandé à PositiveSingles de les enlever de ces sites à plusieurs reprises, mais que l'organisation n'avait pas accédé à leur demande.

Ils ont par conséquent déposé une plainte auprès du Commissariat contre PositiveSingles et son propriétaire, SuccessfulMatch.

Constatations

SuccessfulMatch, qui possède et exploite PositiveSingles.com, est un centre d'affaires pour les entrepreneurs Web qui souhaitent établir des sites Web affiliés. PositiveSingles.com et SuccessfulMatch.com affichent tous deux une adresse et un numéro de téléphone dans la région de Toronto.

Selon sa page d'accueil, PositiveSingles serait « le meilleur et le premier site de rencontre en ligne dans le monde pour les personnes atteintes des affections suivantes : herpès, papillomavirus, VIH/sida, hépatite, chlamydia, gonorrhée, syphilis et autres MTS, en plus d'être complètement anonyme et le plus fiable » [traduction].

Pour sa part, SuccessfulMatch exploite aussi de nombreux autres réseaux de rencontre, ciblant généralement des personnes présentant des caractéristiques démographiques et ayant des intérêts particuliers. Lorsqu'une tierce partie, tel un entrepreneur Internet, achète un nom de domaine pour un réseau de rencontre donné, SuccessfulMatch établit un site Web affilié pour ce domaine et héberge le site.

SuccessfulMatch est responsable des activités liées au site affilié, y compris du logiciel de rencontres, de la base de données des adhérents, du traitement des paiements et de l'assistance technique. L'organisation nous a en outre informés qu'un affilié pouvait seulement voir la page d'accueil de son propre domaine; il ne peut pas accéder au profil ou aux renseignements personnels d'un client sur son propre site ou sur le site principal du réseau. Au cours de notre enquête, nous n'avons relevé aucun élément de preuve contredisant cette affirmation.

SuccessfulMatch nous a dit que les sites Web affiliés étaient en fait des « extensions » du réseau de rencontre principal et constituaient des « portes » donnant accès à la même communauté.

Pour le réseau PositiveSingles, « PositiveSingles.com » est le site principal et gère aussi la base de données des adhérents pour ce site et tous les sites affiliés du réseau de PositiveSingles. Le réseau est aussi censé « alimenter » les différents sites Web affiliés, mais nous avons constaté que les sites ne fournissaient aucune indication quant à la manière dont cette alimentation se faisait ou en quoi elle consistait. De plus, nous n'avons pas pu déterminer le nombre d'affiliés et ce qu'ils représentaient; SuccessfulMatch nous a informés que le nombre d'affiliés fluctuait constamment au gré de la création et de la suppression des sites.

Nous avons exploré ces liens pour déterminer si SuccessfulMatch avait communiqué les renseignements personnels des plaignants à des sites Web tiers comme les plaignants le prétendaient. Les plaignants estimaient que le fait même que leurs profils se soient retrouvés sur de nombreux autres sites laissait supposer une communication non autorisée.

En fait, même si les noms de domaine des sites affiliés appartiennent à de tierces parties, les affiliés ne recueillent aucun renseignement, ne peuvent pas accéder au site affilié lié à leur nom

de domaine et ne peuvent pas agir sur celui ci. De son côté, SuccessfulMatch recueille et agit sur les renseignements présents dans sa base de données.

Notre enquête a donc permis d'établir que SuccessfulMatch n'avait pas communiqué les renseignements à une tierce partie indépendante; PositiveSingles a plutôt utilisé les renseignements provenant des sites affiliés (et de son propre site PositiveSingles.com) pour générer une base de données unique et intégrée.

Par conséquent, nous avons axé notre enquête sur la question de savoir si SuccessfulMatch avait obtenu le consentement des plaignants pour utiliser leurs renseignements de cette manière, sur la question de savoir si les renseignements étaient suffisamment protégés et sur l'utilisation de fichiers témoins sur le site.

Nos conclusions

- **Consentement**

Un bouton intitulé « Comment nous protégeons votre vie privée » [traduction] apparaît bien en vue sur la page d'accueil de PositiveSingles.com. Il conduit à une page remplie de garanties sans réserve de protection de la vie privée et de confidentialité pour les membres du site. Nous avons estimé qu'un utilisateur pouvait facilement confondre cette page avec la politique du site en matière de protection de la vie privée, même si SuccessfulMatch l'utilise comme un outil de marketing pour attirer des personnes qui, du fait de leur problème de santé, accordent une grande valeur à la protection de leur vie privée.

La véritable politique de confidentialité et la convention de services, qui doivent être lues en parallèle pour comprendre les répercussions éventuelles sur la protection de la vie privée, apparaissaient en tant qu'hyperliens dans une police de petite taille au bas de la page d'accueil et de la page « Comment nous protégeons votre vie privée » [traduction]. De plus, ces documents clarifiaient à peine ce qu'il advient des renseignements personnels des individus qui adhèrent à PositiveSingles.

En effet, étant donné que PositiveSingles semblait être un site autonome et était présenté comme tel, les membres potentiels ne pouvaient ordinairement conclure que leurs profils seraient utilisés par un réseau de sites affiliés ou incorporés à une base de données plus vaste.

En somme, nous avons constaté que PositiveSingles projetait une attitude bienveillante qui pouvait générer chez les membres une attente raisonnable, à savoir que leurs renseignements personnels confidentiels seraient bien protégés. Or, ces renseignements personnels ont été largement mis à la disposition d'un réseau de sites Web susceptibles de changer à tout moment, à l'insu des membres.

Nous avons conclu qu'il n'était pas possible pour une personne de raisonnablement comprendre comment ses renseignements personnels pourraient être utilisés ou communiqués. Ainsi, nous avons conclu que SuccessfulMatch n'avait pas respecté le principe de transparence énoncé dans la LPRPDE, et que le consentement obtenu de la part de membres potentiels concernant l'utilisation de leurs

renseignements personnels ne pouvait pas être considéré comme valable.

- **Mesures de protection**

Étant donné la nature délicate des renseignements personnels et médicaux des membres de PositiveSingles, le respect de la confidentialité est vitale. Il est essentiel que les renseignements personnels des membres soient protégés et communiqués seulement à des personnes connues et approuvées par les membres.

Or, les plaignants ont fourni des preuves à l'effet que les non-membres pouvaient accéder à certains renseignements personnels concernant les membres en effectuant des recherches simples sur un moteur de recherche courant. Il apparaissait donc que les mesures de protection nécessaires n'avaient pas été mises en place, ce qui était également contraire à la LPRPDE.

Toutefois, nous avons par la suite observé que les profils des membres ou leurs pseudonymes ne figuraient pas dans les entrées de blogue du cache des moteurs de recherche Internet, ce qui indiquait que des mesures avaient peut-être été prises en vue de résoudre le problème.

- **Fichiers témoins**

Les fichiers témoins sont de petits bouts de code en langage informatique que des tiers, comme des annonceurs, placent sur les ordinateurs des utilisateurs d'Internet afin de recueillir des renseignements précieux au sujet de l'ordinateur ou de son utilisateur. Les fichiers témoins peuvent être utilisés à différentes fins, comme le suivi des préférences ou des pratiques de navigation des personnes, parfois dans le but de les cibler pour la diffusion d'un contenu publicitaire adapté.

Notre enquête a permis de déterminer que la politique de confidentialité de PositiveSingles fournit des renseignements de base sur l'utilisation des témoins et sur la manière dont les utilisateurs peuvent désactiver la fonction. Elle explique aussi que des annonceurs tiers peuvent placer des fichiers témoins dans le navigateur des utilisateurs, ou lire les fichiers témoins qui s'y trouvent.

Nous avons remarqué qu'aucun renseignement n'était fourni sur les types de fichiers témoins utilisés, ou sur la question de savoir si les fichiers témoins permettaient la communication des renseignements personnels.

Il était écrit sur le site Web de PositiveSingles : « à l'inverse de nombreux autres sites Web, nous ne vendrons jamais votre profil à une entité tierce » [traduction]; cependant, SuccessfulMatch suggérait dans sa politique de confidentialité que l'organisation pouvait faire de la publicité comportementale en ligne, pratique pouvant utiliser des fichiers témoins pour suivre les préférences et les activités de navigation des utilisateurs sur le Web.

Nous avons établi que, si SuccessfulMatch faisait effectivement de la publicité comportementale en ligne, elle devait obtenir le consentement valable des personnes suivies et ciblées. Les lignes directrices du Commissariat sur la pratique prévoient en outre que si les personnes suivies ont un problème de santé de nature hautement délicate, le consentement doit être

exprès, et non pas implicite. Les personnes doivent en fait accepter l'utilisation de leurs renseignements personnels à cette fin.

Nos recommandations

Nous avons adressé les recommandations suivantes à SuccessfulMatch dans un rapport d'enquête préliminaire, qui a été achevé en octobre 2012.

- Les utilisateurs doivent savoir d'emblée que les renseignements contenus dans leur profil seront versés dans une base de données à laquelle auront accès d'autres sites de rencontre affiliés à PositiveSingles et qui s'adressent à des personnes ayant des problèmes de santé variés et présentant différentes caractéristiques démographiques. De plus, ils doivent être informés qu'ils ne pourront pas savoir quels sont ces sites Web, et qu'ils ne pourront pas retirer leur profil de ces sites.

  La politique de confidentialité du site Web doit expliquer comment les renseignements sont utilisés par SuccessfulMatch par l'entremise de ses sites affiliés.

- Le lien entre SuccessfulMatch.com et PositiveSingles.com doit être clair, visible et explicite pour les utilisateurs.

- La distinction entre sites « tiers » et sites « affiliés » doit être claire, visible et explicite pour les utilisateurs.

- Nous avons aussi recommandé que SuccessfulMatch explique en détail au Commissariat comment les renseignements personnels des membres inscrits sont protégés sur PositiveSingles, y compris toute mesure technique et tout protocole servant à empêcher le piratage ou à éviter que les personnes non inscrites puissent voir les renseignements personnels publiés sur le site et sur les sites affiliés.

- Nous avons aussi demandé des explications détaillées sur l'utilisation des fichiers témoins par SuccessfulMatch. Si les témoins servent à suivre le comportement en ligne pour des annonceurs tiers, le site doit permettre aux personnes de donner leur consentement exprès et éclairé ou de refuser de le faire.

Que s'est-il passé ensuite?

SuccessfulMatch a répondu à nos recommandations en prenant les mesures suivantes :

- L'organisation a modifié les pages d'accueil et d'inscription du site PositiveSingles pour indiquer que tous les profils créés sur PositiveSingles.com peuvent être vus par les utilisateurs des autres sites Web affiliés au réseau PositiveSingles.

- Même si les renseignements qui apparaissent dans les profils des utilisateurs peuvent être vus sur d'autres sites Web affiliés appartenant au réseau exploité par

SuccessfulMatch, l'organisation a confirmé que les profils n'étaient pas partagés entre ses divers réseaux. L'organisation a modifié sa convention de services en conséquence.

- La politique de confidentialité et d'autres sections du site SuccessfulMatch ont été modifiées afin de mieux expliquer le lien entre SuccessfulMatch, PositiveSingles et la grande « famille d'entreprises qui [...] comprend de nombreux autres sites Web [...] » [traduction].

- L'organisation a modifié sa politique de confidentialité pour inclure des définitions claires et mieux expliquer la nature et la fonction des sites affiliés, et comment ils se rapportent à PositiveSingles et à SuccessfulMatch.

- L'organisation a également reformulé la politique de confidentialité de PositiveSingles pour clarifier la différence entre sites « tiers » et sites « affiliés ».

- SuccessfulMatch nous a informés des mesures de protection qu'elle avait mises en place pour protéger les renseignements personnels des membres et éviter que les données relatives aux utilisateurs apparaissent dans les résultats des moteurs de recherche. Ces mesures sont, notamment, la vérification par mot de passe, le contrôle des données des fichiers journaux des utilisateurs, l'utilisation de coupe feux et le cryptage.

- SuccessfulMatch a modifié sa politique de confidentialité pour expliquer plus clairement les fins pour lesquelles des fichiers témoins sont utilisés. L'organisation a informé le Commissariat qu'elle n'autorisait pas la publicité sur son site, qu'elle n'utilisait pas les fichiers témoins pour faire de la publicité comportementale et qu'elle ne transmettait pas les informations contenues dans les fichiers témoins aux annonceurs.

Nous croyons que les modifications apportées au site PositiveSingles sont importantes. La transparence accrue permettra aux utilisateurs de consentir en meilleure connaissance de cause à l'utilisation de leurs renseignements personnels sur le réseau de sites PositiveSingles. Ainsi, ils auront une plus grande maîtrise de leur réputation en ligne.

Par conséquent, nous avons conclu que la plainte était ***fondée et résolue***.

Selon un sondage, les Canadiennes et Canadiens craignent d'afficher des renseignements personnels en ligne

Un sondage auprès de la population canadienne commandé par le Commissariat à la fin de 2012 a révélé que de nombreuses personnes craignaient beaucoup d'afficher des renseignements les concernant en ligne. En effet :

- 55 % des répondants ont déclaré qu'ils hésitaient beaucoup à révéler leur emplacement sur Internet;
- environ la moitié des personnes interrogées craignaient de publier leurs coordonnées ou des photos ou vidéos personnelles;
- plus de quatre répondants sur dix redoutaient de communiquer des renseignements sur leurs activités sociales.

En tout, seul un répondant sur huit a déclaré que le fait d'avoir affiché des renseignements en ligne avait eu un effet négatif quelconque sur sa vie; cependant, la proportion de personnes qui ont affirmé que l'affichage de renseignements les concernant par elles-mêmes ou par quelqu'un d'autre leur avait nui était presque deux fois plus élevée (26 %) chez les jeunes répondants (âgés de 16 à 24 ans). Les jeunes ont tendance à utiliser davantage la technologie et d'être moins inhibés dans le cyberespace que leurs parents ou grand-parents.

Le sondage, dernier d'une série visant à prendre le pouls de la population canadienne sur la protection de la vie privée, a été publié au printemps 2013. De plus amples détails seront inclus dans le prochain rapport annuel.

1.3 MISE À JOUR D'UNE ENQUÊTE : *Le nouveau propriétaire du site de réseautage social Nexopia s'engage à régler tous les problèmes liés à la protection de la vie privée*

Notre enquête, amorcée il y a trois ans, sur des plaintes se rapportant à un site canadien de réseautage social destiné aux jeunes n'avait toujours pas abouti à un règlement définitif en 2012. Après avoir saisi les tribunaux de cette question, nous avons constaté que l'entreprise avait été mise en vente au milieu de la procédure judiciaire. Le nouveau propriétaire s'étant engagé à adopter toutes les mesures que nous avons recommandées, nous espérons toutefois parvenir à un règlement en 2013.

Notre rapport annuel de 2011 présentait les résultats d'une enquête approfondie sur les pratiques en matière de protection de la vie privée de Nexopia.com.

Nexopia, entreprise fondée en 2003 à Edmonton, se distingue de Facebook et des derniers venus sur la scène du réseautage social en se positionnant comme une « communauté ouverte » d'utilisateurs qui peuvent « communiquer avec leurs amis en ligne et se mettre en valeur aux yeux du monde » [traduction].

Notre enquête, réalisée à la suite d'une plainte déposée par le Centre pour la défense de l'intérêt public, situé à Ottawa, a permis de découvrir que Nexopia contrevenait à plusieurs aspects de la LPRPDE. Nous avons formulé 24 recommandations quant à des mesures correctives à prendre.

Vingt de ces recommandations portaient sur des questions liées à : la divulgation des profils d'utilisateurs au public; aux paramètres de confidentialité par défaut; à la collecte, à l'utilisation et à la communication des renseignements personnels demandés à l'inscription; à la communication de renseignements personnels à des annonceurs et à d'autres tierces parties; à la conservation de renseignements personnels de non utilisateurs.

Nexopia s'est engagée à mettre en œuvre 20 de ces recommandations, dont la plupart d'ici le 30 juin 2012, et les autres au plus tard le 30 septembre 2012. Par conséquent, nous avons jugé que ces aspects de la plainte étaient ***fondées et conditionnellement résolues***.

Cependant, Nexopia a refusé d'adopter les quatre autres recommandations ou d'offrir des solutions de rechange acceptables. Ces recommandations se rapportaient à la conservation indéfinie des renseignements personnels des utilisateurs, même après qu'un utilisateur ait sélectionné l'option de suppression d'un compte, ainsi qu'à l'absence d'un mécanisme de suppression permanente des renseignements personnels enregistrés dans les archives de l'organisation.

Nous avons conclu que ces questions étaient ***fondées*** et qu'elles demeuraient non résolues.

Demande à la Cour fédérale

Le 13 avril 2012, le Commissariat a demandé à la Cour fédérale de rendre une ordonnance obligeant Nexopia à cesser de conserver les renseignements personnels pendant une période indéterminée et à mettre en place une fonction de suppression permettant l'élimination permanente des renseignements personnels des utilisateurs de son site Web, à leur demande, ou lorsque ces renseignements ne sont plus nécessaires pour la réalisation des fins pour lesquelles ils ont été recueillis. (*Commissaire à la protection de la vie privée du Canada c. Nexopia.com Inc.*, dossier de la Cour fédérale n° T 764 12).

Le 30 septembre 2012, Nexopia a été vendue à une autre entreprise. Le nouveau propriétaire s'est engagé à donner suite aux 24 recommandations avant le 30 avril 2013.

Au moment de la rédaction du présent rapport, nous nous affairions à évaluer l'implémentation de nos recommandations par Nexopia.

Conseils à l'intention des joueurs

En septembre dernier, nous avons publié une fiche d'information pour aider les adeptes de jeux en ligne à comprendre les paramètres de confidentialité et à faire des choix éclairés lorsqu'ils jouent à des jeux vidéo sur Internet.

La fiche d'information intitulée *Consoles de jeu et renseignements personnels : la vie privée en jeu* est issue des préoccupations que nous avons entendues dans le cadre de nos consultations publiques menées en 2010 sur l'infonuagique et le suivi en ligne. Des universitaires et des membres du public ont fait remarquer que très peu de conseils sont offerts aux adeptes des jeux vidéo en ligne.

Nous avons donc commencé à nous pencher sur ce phénomène en plein essor. Nous avons testé des consoles de jeu et leurs paramètres de confidentialité. De plus, nous avons examiné des nouvelles fonctions qui lient les activités de jeu à des sites de réseautage social.

Finalement, nous avons mis au point une foire aux questions destinée aux joueurs, petits et grands, ainsi qu'aux enseignants et aux parents. Nous avons rendus publics notre document d'orientation, de même qu'un plan d'apprentissage sur les jeux vidéo élaboré à l'intention des enseignants qui doivent aborder avec les écoliers canadiens des questions liées au monde en ligne.

Consoles de jeu et renseignements personnels : la vie privée en jeu (http://www.priv.gc.ca/information/pub/gd_gc_201211_f.pdf)

1.4 AVANCEMENT DES CONNAISSANCES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE EN LIGNE

L'un des principaux volets du mandat du Commissariat est de faire avancer les connaissances quant aux moyens de mieux promouvoir et défendre le droit à la vie privée. Au fil des ans, nous avons mis au point une stratégie de recherche dynamique et prospective que nous mettons en œuvre non seulement au sein de notre organisation, mais également par l'entremise de notre fort prisé Programme des contributions.

Depuis 2004, le Programme des contributions a financé des travaux novateurs sur un éventail de questions liées à la vie privée. Voici un aperçu de projets qui ont été financés dans le cadre du Programme et qui concernent la vie privée en ligne et ses répercussions sur la réputation des personnes :

- « Jeunes Canadiens dans un monde branché » est un projet à long terme mené par **HabiloMédias** (autrefois le Réseau Éducation Médias) qui a été lancé en 2000. Il vise à recenser et à examiner les comportements, attitudes et opinions des enfants et des adolescents canadiens à l'égard de l'utilisation d'Internet. La phase III du projet, qui est actuellement en cours, comprend un sondage réalisé à l'échelle nationale auprès de 6 000 jeunes, âgés de 9 à 17 ans, pour explorer leurs points de vue sur les importantes nouveautés technologiques et sociales dans le cyberespace. Un

élément clé consiste à examiner les façons dont les jeunes Canadiennes et Canadiens gèrent leurs renseignements personnels, leur vie privée et leur réputation dans le monde en ligne.

- ***L'Association sur l'accès et la protection de l'information*** a élaboré en 2012 une trousse pédagogique destinée aux élèves du premier cycle des écoles secondaires pour les aider à acquérir de bonnes pratiques de protection de la vie privée au moment d'afficher en ligne leurs photographies et leurs renseignements personnels. Le projet présente des outils et des idées pour inciter les jeunes à se montrer soucieux de leur réputation en ligne. La trousse aidera également les enseignants à discuter en classe de la protection de la vie privée et des renseignements personnels en ligne.

Le Programme des contributions a financé 11 projets en 2012-2013 et nous pensons que certains de ces résultats permettront de mettre davantage en lumière les problèmes liés à la vie privée et à la réputation en ligne, surtout en ce qui concerne les appareils mobiles.

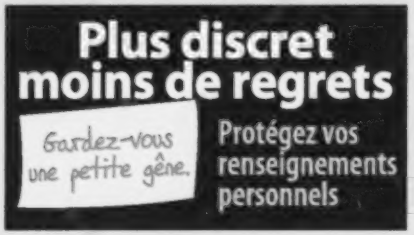
Une description plus détaillée des activités du Programme réalisées en 2012 figure à la section 3.5.1 de ce rapport.

Journée de la protection des données

Le 28 janvier 2012, le Commissariat s'est joint aux gouvernements, aux professionnels de la protection de la vie privée, aux entreprises, aux universitaires et étudiants du monde entier pour célébrer la Journée de la protection des données.

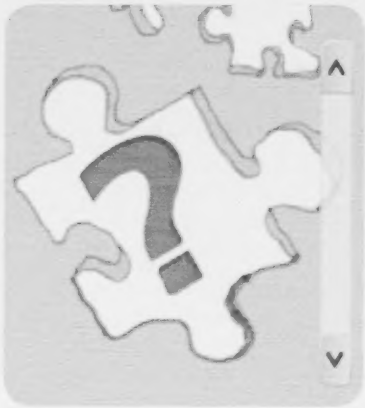
Dans le cadre de cet événement annuel de sensibilisation, nous avons tâché d'inciter les Canadiennes et Canadiens à limiter la quantité de renseignements personnels qu'ils communiquent en ligne. Nous avons utilisé la formule « Plus discret, moins de regrets : Gardez vous une petite gêne » pour signifier que toute chose n'est pas bonne à partager, et tenter d'aider les personnes à réduire leur visibilité sur le Web, de manière à limiter les risques d'une utilisation inappropriée ou d'une divulgation sans leur consentement de leurs renseignements personnels.

Nous avons également encouragé les entreprises à penser en fonction du principe « Plus discret, moins de regrets » au moment de recueillir et de conserver les renseignements personnels des clients. Après tout, plus elles recueillent de renseignements, plus le risque est grand de contrevenir à la LPRPDE.



Pourquoi la responsabilité vous revient

Sur le bureau du président américain Harry S. Truman était placée une plaque qui annonçait fièrement : « *The buck stops here!* » (Le responsable, c'est moi!). L'homme qui a dirigé l'Amérique au cours de sept années tumultueuses, à partir de 1945, voulait que le monde entier sache qu'il était le décideur. Il était le patron et pouvait prendre des décisions difficiles. En un mot, il était vu comme responsable.



En matière de vie privée, le message affiché par Truman pourrait également s'appliquer aux organisations. Au cours de la douzaine d'années qui se sont écoulées depuis l'entrée en vigueur de la LPRPDE, nous constatons que les entreprises se délestent encore beaucoup trop de leurs responsabilités. Trop souvent, elles présument que la tâche d'élaborer des politiques de confidentialité, de les communiquer au personnel et de veiller à ce qu'elles soient comprises et appliquées est l'affaire de quelqu'un d'autre; ou, si elles reconnaissent qu'il s'agit de leur travail, elles n'y pensent qu'après coup et y accordent une importance secondaire par rapport aux activités principales de l'entreprise.

Ce n'est pas le cas. La responsabilité est le premier principe relatif à l'équité dans le traitement de l'information énoncé dans l'annexe 1 de la LPRPDE. De façon très générale, le principe de la responsabilité prévoit qu'une organisation est responsable de ses actions sur le plan éthique. Plus précisément, il confère aux entreprises une obligation juridique de protéger les renseignements personnels qu'elles ont entre les mains.

Les organisations responsables devraient disposer d'un programme sur mesure pour gérer et protéger les renseignements personnels qu'elles détiennent. Ce chapitre décrit le contenu d'un document d'orientation exhaustif que nous avons publié en 2012, de concert avec nos homologues de l'Alberta et de la Colombie-Britannique, provinces qui appliquent des lois essentiellement similaires à la loi fédérale pour le secteur privé. Le document intitulé *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité* guide les organisations dans leurs efforts pour mettre en place une politique en matière de protection de la vie privée qui s'applique à leurs activités.

Les organisations ont tout intérêt à mettre en place un programme efficace de gestion de la protection de la vie privée, pour leurs clients, certes, mais aussi pour elles-mêmes. En effet, nous sommes trop souvent appelés à enquêter sur des dossiers d'entreprises qui ont rendu leurs clients furieux par leur approche nonchalante en matière de protection de la vie privée.

Certainement, cela ne peut pas être bon pour les affaires. Il est temps pour chacun de prendre ses responsabilités.

Dans le présent chapitre

Ce chapitre explore la notion de responsabilité en matière de protection de la vie privée — les situations où cela a fonctionné ou échoué, et ce qui est fait pour la renforcer.

Il présente le sommaire de dossiers sur lesquels nous avons enquêté en vertu de la LPRPDE, qui portaient principalement sur des questions de responsabilité quant au traitement approprié de renseignements personnels. Dans un cas, l'enquête a été réalisée dans le cadre d'une collaboration sans précédent avec notre homologue des Pays Bas.

Mais nous avons fait plus que simplement pourchasser les fautifs; nous avons aussi prêché en faveur de la prévention. Après tout, les entreprises qui comprennent les règles sont plus à même d'éviter les pièges en matière de protection de la vie privée.

Aussi, ce chapitre débute par le résumé d'un nouveau document d'orientation que nous avons publié cette année pour aider les entreprises à mieux s'acquitter de leurs responsabilités en vertu de la LPRPDE.

2.1 LIGNES DIRECTRICES EN MATIÈRE DE RESPONSABILITÉ

Conformément au principe de responsabilité de la LPRPDE, les organisations sont tenues d'accepter la responsabilité de protéger les renseignements personnels qu'elles détiennent. À cette fin, elles doivent disposer de politiques et de procédures visant à promouvoir de bonnes pratiques. Prises ensemble, ces mesures constituent un programme de gestion de la protection de la vie privée.

Bien que la responsabilité soit enchâssée dans la loi canadienne sur la protection des renseignements personnels, nous continuons de nous heurter à des problèmes de responsabilité plutôt élémentaires. Dans nos enquêtes, par exemple, il est souvent difficile d'identifier la personne responsable de la protection de la vie privée dans une organisation, tout comme de savoir si la politique d'une entreprise en cette matière a déjà fait l'objet d'une mise à jour.

Plus récemment, nous avons aussi noté que certaines organisations ne prenaient pas soin d'intégrer un dispositif de protection de la vie privée à leurs produits et services. Même lorsque des politiques étaient en place, il semblait que les concepteurs de programmes et les techniciens informatiques — dont le travail peut potentiellement avoir une incidence considérable sur les renseignements personnels —

n'avaient pas lu ces directives ou ne reconnaissaient pas leur importance.

Nous avons aussi, à notre grande déception, continué de relever certaines atteintes de base à la protection des renseignements personnels, dans des situations où l'inattention des employés ou leur ignorance des bonnes pratiques en matière de protection de la vie privée a donné lieu à des fuites de renseignements personnels qui auraient pu être évitées.

C'est pourquoi au printemps 2012, le Commissariat, en concertation avec ses homologues de l'Alberta et de la Colombie-Britannique, a publié le document *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*.

Un programme de gestion de la protection de la vie privée: la clé de la responsabilité (http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_f.pdf)

Le document d'orientation *La clé de la responsabilité* présente les attentes de nos trois commissariats en matière de programmes de protection de la vie privée. Il souligne la nécessité d'obtenir, de la part des organisations, des engagements et la mise en place de mesures de contrôle des programmes. Puisqu'un programme de protection de la vie privée doit être dynamique et flexible pour s'adapter à l'évolution des besoins et des risques, le document insiste également sur la nécessité d'une évaluation continue et d'une révision.

Notre travail dans ce domaine a été influencé par les changements importants observés à l'étranger. Le Commissariat et les commissaires à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, Jill Clayton et Elizabeth Denham, participent à un débat international sur la notion de responsabilité de l'organisation. L'initiative, dirigée par des entreprises américaines, fait également appel au concours des autorités européennes et nord-américaines de protection des données.

En effet, la responsabilité s'est transformée en un thème général de protection de la vie privée. Les *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données à caractère personnel* de l'Organisation de coopération et de développement économiques ont été, il y a trois décennies, le premier document international à tenir compte du concept. Le Cadre de protection de la vie privée mis au point par la Coopération économique de la zone Asie Pacifique comprend également le principe de responsabilité, et le projet de règlement en matière sur le traitement des données à caractère personnels proposé par la Commission européenne intègre très concrètement la notion de « responsabilité démontrable ».

Les grandes quantités de renseignements personnels, la complexité de leur traitement et la diversité des cadres de protection de la vie privée qui existent dans différents pays expliquent en grande partie cet intérêt croissant pour le concept.

Le Canada ayant depuis longtemps consacré le principe de la responsabilité dans la loi, nos trois

commissariats ont décidé d'étoffer leurs points de vue et d'ajouter leurs voix au débat international en vue d'améliorer le respect de la loi au pays.

Le document a été bien accueilli, suscitant un débat lors de la conférence de l'Association internationale des professionnels de la protection de la vie privée tenue à Bruxelles, ainsi qu'à la réunion du European-American Business Council à Washington; D.C. Un important cabinet d'avocats du pays et le Centre for Information Policy Leadership ont également élaboré des outils pour les clients et les membres en s'appuyant sur le document.

2.2 ENQUÊTE SUR UNE PLAINTE DÉPOSÉE PAR LA COMMISSAIRE : *L'entreprise de location Aaron's utilise un logiciel espion pour retrouver des ordinateurs portatifs*

Contexte

Au début de 2012, nous avons appris que des entreprises de location avec option d'achat œuvrant au Canada auraient utilisé un logiciel espion appelé Detective Mode pour retracer secrètement des ordinateurs portatifs manquants.

Le logiciel, fourni et pris en charge par DesignerWare Inc., une entreprise établie aux États-Unis, pouvait être installé et activé à distance sur les ordinateurs portatifs loués, où il a été conçu pour enregistrer clandestinement les frappes au clavier, les coordonnées, les captures d'écran, les photographies provenant d'une caméra Web et d'autres renseignements. Les données pouvaient être renvoyées à l'entreprise de location pour l'aider à retrouver les ordinateurs portatifs perdus ou volés.

Après consultation avec la Federal Trade Commission des États-Unis, la commissaire a conclu qu'elle disposait de motifs raisonnables pour déposer une plainte à l'encontre d'un franchisé canadien de l'entreprise de location avec option d'achat, Aaron's Inc., grande société cotée en bourse. Ces motifs comprenaient des éléments fiables indiquant que le franchisé avait demandé l'activation du logiciel Detective Mode à 30 reprises au cours d'une période de six mois.

Dans notre plainte, nous avons soutenu qu'une personne raisonnable n'estimerait pas que la recherche d'ordinateurs manquants justifie l'utilisation du logiciel Detective Mode. En outre, nous avons allégué que la nature non ciblée de la surveillance de Detective Mode avait pour résultat la collecte de plus de renseignements qu'il n'était nécessaire pour les fins prévues.

Constatations

Notre enquête a révélé que le franchisé d'Aaron's n'utilisait plus Detective Mode. Toutefois, il l'avait fait dans le passé pour retrouver des ordinateurs portatifs.

L'entreprise a allégué qu'en raison de ses pratiques de suppression des enregistrements, il lui était impossible de déterminer exactement le nombre de fois que Detective Mode avait été utilisé. Cependant, le franchisé a confirmé avoir demandé au moins cinq activations au cours d'une même semaine. Celles ci étaient motivées par la conviction de l'entreprise que le preneur à bail s'était enfui avec l'ordinateur portatif sans effectuer tous les paiements requis.

L'entreprise de location a indiqué que quatre des cinq activations avaient permis de retracer les biens manquants.

Nous avons constaté que les quatre activations fructueuses avaient entraîné la collecte de centaines de pages de documents contenant des renseignements personnels de nature délicate. Nous y avons trouvé notamment la photographie d'un utilisateur prise avec une caméra Web, ainsi que des adresses de courriel, des adresses à domicile, des numéros de téléphone et des messages personnels s'adressant à des membres de la famille et à des amis. Il y avait aussi des captures d'écran de pages de site de réseaux sociaux comprenant des photographies d'enfants, de même que des messages affichés et d'autres données Internet.

Les données ont été recueillies clandestinement à l'aide de la caméra Web de l'ordinateur portatif, de l'enregistrement des frappes au clavier de l'utilisateur et même d'une page fictive d'enregistrement du système d'exploitation.

Aucun des noms et autres coordonnées recueillis de cette manière ne correspondait aux noms des preneurs à bail ayant prétendument disparus avec les ordinateurs portatifs. On ignore de quelle façon ces utilisateurs ont pris possession des ordinateurs portatifs.

Nous avons conclu que l'utilisation non ciblée par l'entreprise du logiciel de surveillance Detective Mode avait entraîné la collecte de plus de renseignements personnels qu'il n'était nécessaire aux fins de la récupération des ordinateurs portatifs.

Qui plus est, on aurait pu avoir affaire à une situation encore pire : Detective Mode est doté de toutes les fonctionnalités voulues pour capter l'image d'un enfant dans sa chambre, ou les codes d'utilisateur et mots de passe d'accès à des comptes bancaires d'un tiers innocent. Une fois le logiciel activé, l'entreprise de location n'a aucune façon de prédire quelles informations elle recueillera.

Nous comprenons que l'entreprise de location soit soucieuse de protéger son inventaire, et que Detective Mode, d'un point de vue technologique, puisse être un outil efficace pour atteindre cet objectif.

Toutefois, nous avons conclu que l'atteinte à la vie privée résultant de cette pratique était excessive et disproportionnée par rapport à l'avantage financier potentiel pour l'entreprise de location. En effet, il est difficile d'imaginer un objectif commercial qui pourrait justifier ce type de collecte non ciblée et clandestine de renseignements personnels.

Que s'est il passé ensuite?

Au vu de nos conclusions, Aaron's a promis de supprimer, dans les plus brefs délais possibles, tous les renseignements personnels restants de ses enregistrements. L'entreprise s'est également engagée à ne plus jamais utiliser ce type de logiciel espion.

Par conséquent, nous avons conclu que notre plainte était ***fondée et résolue***. Nous continuerons de surveiller le marché canadien pour repérer toute utilisation de logiciels semblables.

2.3 ENQUÊTE SUR UNE PLAINTE : *Un assureur utilise les cotes de crédit pour fixer les primes d'assurance, à l'insu des clients*

Contexte

Un couple de l'Ontario a eu la surprise de voir sa prime d'assurance habitation augmenter considérablement entre deux renouvellements de police. Les membres du couple bénéficiaient d'une cote de crédit parfaite depuis 50 ans, mais leur situation a changé au cours de l'année, pendant laquelle ils ont cosigné un prêt pour lequel il y a eu trois défauts de paiement.

La compagnie d'assurances du couple a confirmé qu'un changement soudain dans la cote de crédit de ce dernier était l'un des facteurs à l'origine de l'augmentation de sa prime d'assurance habitation.

Le couple a déposé une plainte auprès du Commissariat qui en a tiré trois principaux éléments.

Constatations

- **Objectifs de la collecte**

Depuis plusieurs années, la compagnie d'assurances envoie un avis détaillé à tous ses titulaires de polices d'assurance ontariens lors du premier renouvellement de leur police d'assurance. L'avis explique que la compagnie reçoit d'une agence d'évaluation du crédit du Canada une cote pour fins d'assurances qui est dérivée du rapport de solvabilité des titulaires de police d'assurance, et qu'elle peut l'utiliser comme un facteur parmi d'autres pour déterminer l'admissibilité à l'assurance habitation et le montant des primes.

Il semblerait que la cote de crédit soit un indicateur de risque, bien que nous ayons constaté que ce point de vue n'est pas partagé unanimement dans l'ensemble de l'industrie des assurances.

En ce qui concerne ce dossier, nous avons conclu qu'une personne raisonnable jugerait acceptable qu'une compagnie d'assurances recueille et utilise les cotes de crédit comme outil de souscription des polices d'assurance et d'établissement des primes.

D'abord, l'évaluation du risque au moyen d'outils de souscription fiables est une composante essentielle du secteur de l'assurance. Cette pratique est avantageuse tant pour les assureurs, qui peuvent ainsi mieux gérer les risques et, par conséquent, établir de manière convenable et concurrentielle le prix de leurs produits d'assurance, et pour les assurés, dont les primes concordent mieux avec leur niveau de risque particulier.

Ensuite, la pratique est parfaitement légale en Ontario. L'article 8 de la *Loi sur les renseignements concernant le consommateur* de la province stipule que les renseignements sur le crédit peuvent être divulgués à des fins de souscription d'assurances. (L'utilisation de renseignements sur le crédit dans le contexte de l'assurance habitation n'est pas permise dans certaines autres provinces, dont Terre-Neuve-et-Labrador.)

Nous avons en outre noté que la cote de crédit étant une donnée agrégée, elle est moins susceptible de porter atteinte à la vie privée que ne l'est l'accès au rapport de solvabilité complet d'une personne.

Par conséquent, nous avons conclu que la plainte ***n'était pas fondée*** en ce qui a trait aux fins de la collecte.

Il convient également de noter que le Bureau d'assurance du Canada a publié des directives concernant l'utilisation des renseignements sur le crédit par les assureurs. Le *Code de conduite sur l'utilisation de l'information de crédit par les assureurs* conseille aux compagnies d'assurances de ne pas utiliser les renseignements sur le crédit comme une variable unique et de ne pas refuser de fournir des soumissions et des polices d'assurance aux clients qui refusent de consentir à ce que leurs renseignements sur le crédit soient utilisés.

- **Consentement**

Le couple, qui était un client de la compagnie d'assurances depuis six ans, ignorait cette pratique et estimait que l'organisation n'avait pas obtenu son consentement explicite pour utiliser ses renseignements sur le crédit.

La compagnie d'assurances, pour sa part, estimait que les plaignants avaient consenti à la collecte de renseignements sur le crédit lors de la signature de leur demande initiale.

Nous avons constaté que les dispositions relatives au consentement du formulaire de demande de la compagnie d'assurances n'étaient pas suffisamment précises pour obtenir le consentement explicite à cette utilisation des renseignements liés au crédit.

Nous ne pouvions pas non plus nous attendre à ce que les clients déduisent aisément cette utilisation, celle ci n'étant ni courante ni escomptée pour ce type de renseignements. En effet, une enquête commandée par les Courtiers d'assurances inscrits de l'Ontario en novembre 2010 a révélé que les trois quarts des consommateurs de l'Ontario n'étaient pas au courant que leurs cotes de crédit étaient utilisées pour déterminer le coût de leurs primes d'assurance habitation.

Nous avons aussi remarqué que le Code de conduite de l'industrie des assurances fournit une procédure détaillée pour l'obtention du consentement lors de

l'utilisation des renseignements relatifs au crédit et recommande clairement d'obtenir un consentement explicite et éclairé.

Nous estimons que la pratique de la compagnie d'assurances qui consiste à envoyer des informations détaillées supplémentaires aux titulaires d'une police d'assurance un an après la signature de leur police initiale n'est pas un moyen d'obtenir un consentement approprié.

Par conséquent, nous avons conclu que le consentement adéquat pour la collecte et l'utilisation de ce type de données n'avait pas été obtenu. En ce qui concerne le consentement, nous avons donc conclu que la plainte était ***fondée***.

- **Transparence**

Le dernier élément de la plainte se rapportait au manque de renseignements explicites mis à la disposition des personnes sur l'utilisation qui était faite de leurs renseignements personnels pour déterminer les primes ou l'admissibilité.

Le sondage effectué par l'industrie ontarienne de l'assurance ayant montré que les trois quarts des consommateurs de l'Ontario ignoraient l'utilisation potentielle qui est faite de leurs cotes de crédit dans l'établissement de leurs primes d'assurance habitation, il n'est pas étonnant que les plaignants disent ne pas avoir été au courant de cette pratique.

En effet, notre enquête a révélé que le site Web de la compagnie n'offrait aucune information explicite sur les pointages statistiques ou l'utilisation qui est faite des renseignements sur les cotes de crédit pour déterminer les primes. Cette information n'était pas non plus incluse dans la politique de confidentialité de la compagnie, accessible en ligne.

Nous avons par conséquent conclu que la plainte était également ***fondée*** en ce qui concerne la transparence.

Que s'est il passé ensuite?

Dans les provinces et territoires qui utilisent les renseignements sur le crédit comme outil de souscription, la compagnie a envoyé un avis révisé à tous ses titulaires de police d'assurance. L'objectif était d'aviser les clients de l'utilisation que l'entreprise fait des renseignements liés au crédit pour évaluer le risque du client.

La compagnie a également mis à jour son site Web pour informer ses clients assurés que les renseignements sur le crédit sont l'un des outils de souscription utilisés pour évaluer le risque lié au client.

En réponse à nos recommandations, l'assureur a aussi accepté de modifier son formulaire de demande de façon à y insérer une disposition sur le consentement à la collecte et à l'utilisation des cotes de crédit. La compagnie s'est en outre engagée à informer le Commissariat une fois que le libellé du texte sur le consentement aurait été modifié.

Nous avons considéré que la plainte était ***conditionnellement résolue*** et nous en assurerons le suivi pour veiller à ce que toutes nos recommandations soient appliquées.

2.4 ENQUÊTE SUR UNE PLAINTE :
Une société de prêts hypothécaires recueille les renseignements personnels d'un couple à son insu et sans son consentement

Contexte

Un courtier en prêts hypothécaires a demandé à une société de prêts hypothécaires (agissant comme administrateur) de préparer une lettre d'intérêt pour le financement d'une hypothèque, renfermant une cote relative à la capacité financière d'un couple de construire une maison sur sa propriété. L'entreprise a préparé la lettre pour le courtier, mais cela s'est fait à l'insu du couple. Le document n'a pas été signé par les plaignants.

À leur grande surprise, les membres du couple ont vu la lettre présentée plus tard dans le cadre d'une poursuite judiciaire qui était en cours et qu'ils avaient intentée contre l'ancien conjoint de l'un d'entre eux, lequel s'était depuis remarié avec le courtier en prêts hypothécaires.

La lettre contenait des quantités importantes de renseignements personnels, dont certains étaient tirés d'un affidavit assermenté par le couple et soumis plus tôt dans le cadre de la poursuite judiciaire. La lettre comprenait aussi d'autres renseignements sur l'historique des ventes de la propriété du couple et ses fonds personnels disponibles pour la construction.

Le couple a été d'autant plus troublé que la lettre se soit retrouvée devant la cour qu'il n'était client ni du courtier en prêts hypothécaires ni de la société de prêts hypothécaires; il n'était pas à la recherche de financement hypothécaire et n'avait jamais demandé de lettre de cette nature.

Le couple a, par conséquent, déposé une plainte auprès du Commissariat.

Constatations

Un porte parole de la société de prêts hypothécaires nous a dit avoir préparé la lettre en toute bonne foi et suivi les lignes directrices en vigueur.

Cependant, il a aussi reconnu avoir cru sur parole le courtier en prêts hypothécaires et ne pas avoir vérifié si le couple avait consenti à la collecte, à l'utilisation et à la communication de ses renseignements personnels à cette fin particulière.

Il a en outre soutenu qu'il ne savait pas que la lettre pourrait être utilisée dans le cadre d'une poursuite judiciaire. Toutefois, il a allégué que certains des renseignements sur le couple étaient accessibles au public et, par conséquent, exclus des exigences de la LPRPDE relativement au consentement.

Nous avons constaté que, lors de la préparation et de l'émission de la lettre d'intérêt pour le financement hypothécaire, la société de prêts hypothécaires avait recueilli, utilisé et communiqué les renseignements personnels du couple à son insu et sans son consentement.

Nous avons aussi conclu que, bien que certains des renseignements figuraient effectivement dans le dossier de la poursuite judiciaire en cours, la société ne pouvait pas supposer qu'ils étaient « accessibles au public » et donc exclus des exigences de la LPRPDE relatives au consentement pour leur communication.

Le règlement d'application de la LPRPDE stipule que les renseignements personnels qui figurent dans un dossier d'un organisme judiciaire ne peuvent être réputés « accessibles au public » que *si la collecte, l'utilisation et la communication de ces renseignements sont directement liées à la raison pour laquelle ils figurent dans le dossier ou document*.

Dans ce cas, nous avons conclu que la raison pour laquelle la société de prêts hypothécaires avait recueilli les renseignements personnels ne se rapportait pas directement à la raison pour laquelle ils figuraient dans le dossier du tribunal.

Par conséquent, le consentement du couple aurait dû être obtenu pour la collecte, l'utilisation et la communication des renseignements contenus dans la lettre.

Que s'est il passé ensuite?

Afin d'éviter qu'une telle situation ne se répète, le Commissariat a recommandé que la société de prêts hypothécaires établisse une procédure pour obtenir le consentement en vue de la collecte, de l'utilisation et de la communication des renseignements personnels. Nous lui avons également suggéré de nous tenir au courant de la mise en œuvre de la procédure.

En guise de réponse, la société de prêts hypothécaires a établi une nouvelle procédure prévoyant que les renseignements personnels ne seraient pas recueillis, utilisés ou communiqués sans le consentement direct de la personne concernée. Dans le cas de renseignements personnels obtenus par l'intermédiaire d'un tiers, la société examinera la pertinence de tout consentement antérieur.

La société a aussi donné une formation sur la nouvelle procédure à son personnel et a élaboré des documents de référence connexes.

Par conséquent, nous avons conclu que la plainte était ***fondée et résolue***.

2.5 ENQUÊTE SUR UNE PLAINTE : *Une agente d'assurance communique des renseignements de nature délicate dans un message laissé sur une boîte vocale*

Contexte

La plaignante était employée dans un salon de coiffure lorsqu'elle a appelé sa compagnie d'assurances pour obtenir un devis d'assurance de responsabilité civile pour un salon de coiffure à la maison qu'elle songeait à ouvrir. On lui a alors répondu qu'une agente la rappellerait pour lui fournir l'information demandée.

Quelques jours plus tard, l'employeur de la plaignante a récupéré un message sur le système de messagerie vocale du salon de coiffure, dans lequel la compagnie d'assurances demandait à la plaignante de la rappeler pour lui fournir plus de renseignements sur l'entreprise qu'elle envisageait d'ouvrir à la maison. Lorsque son employeur l'a confrontée, la plaignante a reconnu qu'elle avait l'intention de quitter le salon dans cinq semaines. Elle a été congédiée dans la semaine qui a suivi.

La plaignante a communiqué avec la compagnie d'assurances pour l'informer de son congédiement et a demandé pourquoi un message détaillé avait été laissé à son lieu de travail, alors qu'elle avait demandé qu'on lui téléphone uniquement à la maison. La compagnie a prétendu ne pas être au courant de cette demande.

Constatations

Nous n'avons recueilli aucune preuve à l'appui de l'allégation de la plaignante selon laquelle elle aurait demandé expressément à la compagnie d'assurances de la rappeler uniquement à la maison. Néanmoins, les parties s'entendent pour dire que la compagnie d'assurances a laissé un message à la plaignante en utilisant son numéro de téléphone au travail.

La compagnie d'assurances ne disposait d'aucune politique précise ayant trait aux messages laissés sur les répondeurs téléphoniques. Lorsque nous lui avons recommandé de mettre en place une telle politique, la compagnie a d'abord refusé.

Nous sommes d'avis que la compagnie d'assurances a communiqué plus de renseignements que nécessaire alors qu'il s'agissait simplement de demander à la plaignante de rappeler l'agente de la compagnie d'assurances. Nous avons également estimé que le message comprenait des renseignements personnels de nature délicate et qu'ils étaient susceptibles d'être interceptés par des personnes autres que la plaignante.

Notre enquête a aussi déterminé que les employés de la compagnie d'assurances étaient tenus de signer une entente de confidentialité et de respecter les dispositions de la LPRPDE. Dans ce contexte, nous avons conclu que l'agente ne devrait pas avoir supposé que la plaignante aurait consenti, même implicitement, à ce que ces renseignements personnels délicats soient communiqués de façon aussi publique.

Dans notre rapport préliminaire, nous avons demandé à la compagnie d'élaborer des politiques visant à réduire le risque que des renseignements personnels sur des clients soient communiqués à des tiers non autorisés lorsque le personnel laisse des messages téléphoniques, et d'offrir aux responsables de la protection de la vie privée et aux employés une formation sur la protection de la vie privée.

Que s'est-il passé ensuite?

Dans sa réponse, la compagnie s'est engagée à mettre en œuvre une nouvelle procédure réduisant au minimum l'information laissée par les employés

dans les messages téléphoniques et nous a fourni un exemple de communications.

La compagnie d'assurances a également modifié les procédures internes en vertu desquelles les coordonnées et les préférences des clients en matière de messagerie doivent être mises à jour.

Par conséquent, le Commissariat a conclu que la plainte était ***fondée et résolue***.

2.6 ENQUÊTE SUR UNE PLAINTE : *Un employé d'une banque commet une erreur en communiquant les données d'un homme à son épouse*

Contexte

Au cours d'une transaction, un employé d'une banque a donné par erreur à une cliente la copie d'un dossier bancaire renfermant le profil financier détaillé de son mari.

Lorsque le mari a appris par son épouse la communication alléguée, il s'est plaint à la banque, ainsi qu'à l'ombudsman des services bancaires et d'investissement.

Insatisfait des réponses obtenues, il a déposé une plainte auprès du Commissariat. Il a allégué que la banque avait révélé ses renseignements personnels à son épouse à son insu et sans son consentement, et que la banque n'avait pas protégé ses renseignements personnels.

Constatations

La banque a convenu qu'un employé avait communiqué les renseignements personnels de nature financière du plaignant sans son consentement à une personne n'ayant pas droit d'obtenir cette information.

Notre enquête a permis d'établir que la banque disposait de mesures de protection procédurales qui semblaient appropriées par rapport au degré de sensibilité des renseignements du plaignant. De plus, nous avons constaté que l'employé avait suivi récemment la formation sur la protection de la vie privée des clients.

Il est cependant évident que l'employé n'a pas appliqué les procédures normalisées de la banque visant à protéger les renseignements personnels des clients. L'employé a notamment omis de suivre les procédures élémentaires d'identification et d'authentification du client, ainsi que de respecter l'exigence selon laquelle les employés doivent signaler les erreurs ou événements touchant des renseignements de clients.

Que s'est il passé ensuite?

À la suite de l'incident, la banque a rappelé aux employés visés par la plainte l'importance de protéger la confidentialité des renseignements des clients, ainsi que les politiques et procédures de la banque en matière de protection de la vie privée.

Par conséquent, nous avons conclu que la plainte liée à la communication de renseignements personnels était fondée. Nous avons déterminé que la plainte liée aux mesures de protection de la banque en ce qui a trait aux renseignements personnels était ***fondée et résolue***.

En guise de conclusion

Ce cas démontre que les politiques et les procédures de protection, bien qu'essentielles, ne suffisent pas, seules, à assurer la protection des renseignements personnels contre une communication non autorisée. L'efficacité des mesures de protection dépend ultimement de leur mise en œuvre diligente et cohérente.

Compte tenu des plaintes répétées de communication inappropriée de renseignements personnels que nous avons reçues à l'encontre de la banque, nous lui avons conseillé vivement de revoir et de renforcer ses programmes de formation des employés et sa gouvernance interne.

Nous l'avons, en particulier, encouragée à consulter le document d'orientation *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité* (voir la section 2.1), pour garantir l'application au sein de la banque des éléments de la structure de gouvernance.

2.7 ENQUÊTE COLLABORATIVE SUR UNE PLAINTE : *WhatsApp Messenger prend des mesures pour atténuer les risques d'atteinte à la vie privée dans son application mobile*

Contexte

Le service de messagerie de WhatsApp, appelée « WhatsApp Messenger », est une application pour téléphone intelligent qui permet aux personnes d'échanger instantanément des messages sur leurs appareils mobiles à l'aide d'un service de transmission de données (Internet), plutôt qu'un service de téléphonie. Cette fonction le distingue des services de communication textuelle ou service de messages courts (SMS) utilisés généralement dans les téléphones cellulaires et les téléphones intelligents. En plus de la messagerie de base, l'application permet aux utilisateurs d'envoyer et de recevoir des images, ainsi que des messages vidéo et audio.

La messagerie de WhatsApp permet aussi aux utilisateurs de communiquer avec différentes familles d'appareils mobiles, notamment les BlackBerry, les iPhone, les téléphones utilisant Windows ou Android — une fonction qui n'est généralement pas disponible sur les systèmes propriétaires de messagerie que les fabricants intègrent à leurs propres téléphones. Toutefois, l'expéditeur et le destinataire d'un message doivent installer l'application et s'inscrire à WhatsApp.

Au début de 2012, la messagerie de WhatsApp était l'une des cinq principales applications mobiles les plus vendues dans le monde et était largement utilisée par les Canadiennes et Canadiens. Selon certaines estimations, plus d'un milliard de messages par jour

ont été transmis par les abonnés de WhatsApp dans le monde entier.

La commissaire Stoddart, toutefois, avait des motifs raisonnables de se préoccuper de la façon dont WhatsApp Inc., entreprise située en Californie et exploitant de l'appli, recueillait, utilisait, communiquait et conservait les renseignements personnels. Elle a déposé une plainte en matière de protection de la vie privée en janvier 2012.

Entre temps, l'autorité néerlandaise de protection des données, le *College bescherming persoonsgegevens*, a aussi émis quelques réserves quant à l'incidence de la technologie et nous a consultés pour obtenir notre point de vue. En raison de la portée internationale de la technologie, et parce que les questions de protection de la vie privée à l'échelle internationale exigent de plus en plus une réponse internationale, le Commissariat et l'autorité néerlandaise ont décidé de mener des enquêtes distinctes, mais coordonnées.[1]

Constatations

L'enquête a révélé que WhatsApp contrevenait aux principes canadiens et aux principes mondialement reconnus en matière de protection de la vie privée, principalement en ce qui concerne la conservation, la protection et la communication de renseignements personnels.

- **Conservation**

Pour fonctionner, WhatsApp doit communiquer avec d'autres appareils mobiles dont les numéros sont enregistrés chez WhatsApp. Nous avons donc examiné la façon dont les numéros de téléphone mobiles d'autres utilisateurs de WhatsApp sont ajoutés à la liste de contacts d'un utilisateur de WhatsApp.

Nous avons constaté que l'application récupère les données du carnet d'adresses sur l'appareil mobile de l'utilisateur. Une fois qu'un utilisateur a autorisé l'application à accéder à son carnet d'adresses, des renseignements particuliers enregistrés dans l'appareil mobile sont périodiquement transmis à WhatsApp pour faciliter l'identification d'autres utilisateurs de WhatsApp.

Ce processus, cependant, récupère aussi les numéros de téléphones mobiles des personnes qui ne sont pas des abonnés de WhatsApp. Qui plus est, nous avons découvert que WhatsApp conserve ces numéros soi disant « hors réseau ». Bien que les numéros soient stockés sous une forme protégée, la pratique enfreint néanmoins un important principe de protection de la vie privée, qui prévoit qu'on ne peut conserver les renseignements qu'aussi longtemps qu'ils sont nécessaires aux fins déterminées.

- **Protection**

Au début de notre enquête, les messages envoyés au moyen du service de messagerie de WhatsApp n'étaient pas cryptés et risquaient, par conséquent, d'être lus clandestinement ou interceptés, surtout

[1] Pour de plus amples renseignements sur cette initiative de collaboration internationale, consultez la section Initiatives mondiales du chapitre 4.

lorsqu'ils étaient envoyés à partir de réseaux Wi Fi non protégés.

En septembre 2012, en partie pour donner suite à notre enquête, WhatsApp a commencé à utiliser le cryptage pour son service de messagerie mobile.

Au cours de notre enquête, nous avons également remarqué que WhatsApp générait des mots de passe pour l'échange de messages en utilisant des renseignements associés aux appareils mobiles, qui peuvent être assez facilement exposés. À cause de cette pratique, il y avait un risque qu'un tiers envoie et reçoive des messages au nom des utilisateurs à l'insu de ces derniers.

À la suite de nos recommandations, WhatsApp a renforcé son processus d'authentification au moyen d'un système plus sécuritaire de mots de passe générés d'une manière aléatoire. Au moment où notre enquête s'achevait, les mesures de sécurité utilisées par WhatsApp semblaient correspondre au degré de sensibilité des renseignements personnels exposés au risque.

Néanmoins, nous avons encouragé WhatsApp à continuer de faire preuve de vigilance en ce qui a trait à la protection des renseignements personnels, étant donné que le contexte de menace est en constante évolution.

- **Limitation de la communication**

Une autre question portait sur les mises à jour du « statut » que les utilisateurs choisissent de partager avec d'autres. WhatsApp permet aux utilisateurs d'entrer et de partager des messages relatifs à leur statut, dont la longueur est limitée à 139 caractères. Les messages courants de statut comprennent « *available* » (disponible), « *busy* » (occupé), « *at school* » (à l'école), « *at work* » (au travail), « *sleeping* » (en train de dormir), « *in a meeting* » (en réunion) et « *urgent calls only* » (appels urgents seulement).

Une fois saisi et sauvegardé, le statut d'un utilisateur, qui peut renfermer des renseignements personnels, est diffusé à tous les utilisateurs de WhatsApp qui ont le numéro de téléphone mobile de l'utilisateur.

À notre avis, toutefois, la diffusion potentiellement non ciblée des messages de statut ne correspondait pas aux attentes raisonnables des utilisateurs. Ces derniers ne pouvaient pas correctement limiter ou agir sur les destinataires de ces messages.

À la suite de notre enquête, WhatsApp a accepté de mieux informer les utilisateurs, pour qu'ils comprennent que leurs messages de statut seront diffusés à grande échelle. À titre d'exemple, l'organisation s'est engagée à mettre en place des avertissements en temps réel, tels que des fenêtres contextuelles, dans les versions futures de l'application.

Le Commissariat n'a pas le pouvoir de rendre des ordonnances. Cependant, WhatsApp a exprimé une volonté de se conformer à nos recommandations dans un délai raisonnable. Nous continuerons à suivre les progrès de l'entreprise dans la mise en œuvre des engagements pris au cours de notre enquête.

Document d'orientation sur les applis mobiles

La popularité croissante des téléphones intelligents, des tablettes et d'autres technologies de communications mobiles a donné naissance à tout un nouveau monde d'applications mobiles, ou applis, telles que les outils de référence et les jeux.

Les applis font maintenant largement partie de notre quotidien. Elles nous guident vers le café le plus proche, nous mettent en communication avec des amis (et même avec de parfaits étrangers), nous divertissent et nous amusent, et nous permettent de régler sure le champ les chicanes entre amis.

Mais elles comportent leur lot de risques. Il y a toujours une possibilité que quelqu'un accède sans autorisation à vos données personnelles, telles que votre carnet d'adresses ou vos photos.

Certaines applis sont également munies de capteurs de mouvements qui peuvent suivre vos déplacements. Grâce à cette information jumelée aux données sur vos activités et préférences, il est possible de brosser assez précisément votre portrait — à votre insu et sans votre consentement.

Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée (http://www.priv.gc.ca/information/pub/gd_app_201210_f.asp)

Songez comment il est difficile, par exemple, pour un concepteur de logiciels de communiquer à l'utilisateur d'un ordinateur conventionnel de bureau de l'information sur la protection de ses renseignements personnels. Ajoutez y les défis que représentent un petit écran et l'attention intermittente d'un utilisateur d'appareil mobile moyen.

À cette difficulté s'ajoute la vitesse ultrarapide du cycle de développement des applis : une nouvelle appli est prête à être téléchargée bien avant que vous n'ayez eu le temps d'étudier l'incidence sur la vie privée de la précédente.

C'est pour cette raison que le Commissariat a collaboré avec ses homologues de l'Alberta et de la Colombie-Britannique pour publier un nouveau document d'orientation pour les concepteurs d'applis en octobre dernier. Dans le document intitulé *Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée*, nous avons voulu que les concepteurs comprennent qu'il est dans leur intérêt de protéger la vie privée. Nous sommes convaincus que les applis mobiles qui tiennent compte de la vie privée seront celles qui se distingueront de la concurrence et gagneront la confiance et la loyauté des utilisateurs.

Il convient de noter qu'une enquête menée en 2012 par le Pew Research Center, groupe de réflexion situé à Washington, D.C., a révélé que 57 % des utilisateurs d'applis aux États-Unis ont soit désinstallé une appli en raison d'inquiétudes liées à la nécessité de partager leurs renseignements personnels ou carrément refusé d'installer une appli pour des raisons similaires.

Nous nous sommes concentrés sur cinq domaines importants que les concepteurs d'applis doivent prendre en considération, notamment une liste de contrôle à suivre et d'autres ressources pour veiller à ce qu'ils aient tous les renseignements voulus pour intégrer la protection de la vie privée à l'étape de la conception.

2.8 ENQUÊTE SUR UNE PLAINTE : *Une entreprise de télécommunications ne respecte pas ses propres politiques relatives aux demandes d'accès aux renseignements personnels*

Contexte

Une femme se trouvant mêlée à un différend de facturation avec une entreprise de télécommunications après l'annulation de son compte de services Internet et sans-fil a demandé à l'entreprise de lui remettre toutes les notes et transcriptions concernant les conversations enregistrées entre elle et la société, pour les mois de février et de mars 2010. Elle soutient que la compagnie n'a pas donné suite à sa demande.

En juillet 2010, la femme a reçu un appel d'une agence de recouvrement. Cet appel l'a incitée à communiquer par courrier recommandé avec le responsable de la protection de la vie privée de l'entreprise de télécommunications, demandant de nouveau l'accès aux notes et aux transcriptions des conversations enregistrées la concernant.

Une entente a fini par être conclue entre elle et le fournisseur de télécommunications, et la facture finale a été payée.

La personne a ensuite reçu un appel d'une autre agence de recouvrement, donnant lieu à une troisième demande d'accès aux conversations enregistrées en février 2011.

Le différend principal a été résolu lorsque l'entreprise de télécommunications s'est excusée de ses agissements, a renoncé au solde du compte et a procédé à la suppression de certaines remarques du rapport du bureau de crédit de la plaignante. La femme a déposé une plainte auprès du Commissariat.

Constatations

Nous avons confirmé que la compagnie de télécommunications avait reçu la première demande d'accès de la plaignante en mars 2010, ainsi qu'une demande subséquente.

L'entreprise a toutefois déclaré que puisque les négociations en vue du règlement du différend avec la plaignante s'étaient déroulées sur une longue période, ses représentants ont cru à tort qu'il n'était pas nécessaire de donner suite à la demande de la plaignante en lui remettant les notes et les transcriptions demandées.

L'entreprise a affirmé avoir pour politique de répondre gratuitement aux demandes de notes et de transcriptions des enregistrements audio dans les 30 jours qui suivent la réception de la demande. Les enregistrements audio sont généralement conservés pendant six mois. Si un enregistrement fait l'objet d'une demande d'accès, il est conservé pendant une période supplémentaire de six mois après l'envoi d'une transcription au demandeur.

Dans le cas qui nous occupe, lorsque la plaignante a fait sa troisième demande d'accès, les anciens enregistrements audio, dont les transcriptions avaient fait l'objet de sa première demande d'accès,

avaient été effacés. Cette situation était contraire aux politiques et aux procédures internes de l'entreprise.

La plaignante n'a pas eu accès à ses renseignements personnels dans le délai de 30 jours prévu aux termes de la LPRPDE, et une prolongation de 30 jours n'a pas non plus été accordée à la plaignante ni demandée par elle. L'entreprise est réputée, par conséquent, avoir refusé de donner suite à la demande d'accès.

Que s'est il passé ensuite?

L'entreprise a répondu à notre rapport d'enquête préliminaire en modifiant sa politique et ses procédures de demande d'accès pour assurer la cohérence de leur contenu.

Elle a reconnu et réaffirmé ses obligations quant au respect des délais précisés dans la LPRPDE.

Elle a également précisé sa politique de conservation des données en ce qui concerne les renseignements personnels qui font l'objet d'une demande d'accès, ainsi que la nécessité de reporter l'échéancier habituel de destruction pendant un certain temps après qu'une réponse ait été donnée à une demande.

En ce qui concerne la formation et la sensibilisation du personnel, le responsable de la protection de la vie privée de l'entreprise a publié une note de service à l'intention des dirigeants et des gestionnaires pour leur rappeler leurs responsabilités en matière de protection de la vie privée et souligner nos préoccupations à l'égard des agissements de l'entreprise.

Il a joint à la note de service une copie des lignes directrices en matière de responsabilité du Commissariat, ainsi qu'une présentation destinée aux dirigeants et aux gestionnaires au sujet des demandes de notes et d'enregistrements audio relatifs à des comptes.

L'entreprise a également confirmé que ces ressources seraient intégrées aux notes d'orientation fournies à tous les employés qui se joignent au service responsable de traiter les demandes d'accès.

À la suite des mesures prises par la société, le Commissariat a conclu que l'affaire était ***fondée et résolue***.

En guise de conclusion

Nous avons encouragé l'entreprise à se familiariser davantage avec nos lignes directrices en matière de responsabilité. Nous avons insisté particulièrement sur la section qui porte sur les mesures de contrôle du programme, qui précise qu'une organisation devrait adopter des mesures de contrôle pour garantir l'application, au sein de l'organisation, des éléments de la structure de gouvernance en matière de protection de la vie privée.

Les lignes directrices soulignent également l'importance de mettre en place des programmes appropriés de formation et de sensibilisation. Par exemple, les employés qui traitent directement les renseignements personnels devraient recevoir une formation supplémentaire adaptée à leurs fonctions particulières. La formation doit aussi être renouvelée, et le contenu mis à jour en fonction des changements.

Présentation d'un mémoire lors des audiences du CRTC à propos du Code sur les services sans fil

En octobre 2012, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a sollicité des commentaires sur sa proposition d'établir un code de conduite obligatoire pour régir les pratiques commerciales des fournisseurs de services de communications sans fil.

Ce code arrive particulièrement à point au vu de la popularité grandissante des téléphones intelligents et d'autres appareils mobiles, et du grand nombre d'entreprises qui adoptent des systèmes de paiements mobiles.

Profitant de l'occasion qui lui était donnée de commenter le code, le Commissariat a soumis un mémoire au CRTC. Nous avons exprimé notre soutien à l'égard de l'élaboration d'un tel code et avons fortement conseillé qu'il soit rédigé de manière à tenir compte des obligations des entreprises en vertu de la LPRPDE.

Nous avons soutenu que le respect de la vie privée est essentiel à la confiance des consommateurs sur laquelle repose l'économie sans fil.

2.9 ENQUÊTE SUR UNE PLAINTE : *Des camps d'été échangent des renseignements sur un enfant sans le consentement parental*

Contexte

Une mère a tenté d'inscrire son enfant à un camp d'été pour la première fois. Nous le désignerons ici comme le « nouveau camp ». La femme a transmis une demande en ligne et s'est entretenue avec le directeur, qui n'a pas accepté tout de suite l'inscription de son enfant.

Lorsque sa demande a été rejetée, la plaignante a déposé une plainte auprès du Commissariat à la fois contre le nouveau camp et un autre camp d'été auquel son enfant avait participé dans le passé, que nous appellerons l'« ancien camp ».

La mère était très vexée et croyait que les renseignements sur son enfant avaient été communiqués d'une façon inappropriée entre les deux camps, contribuant possiblement à la décision du directeur du nouveau camp de ne pas accepter son enfant.

En particulier, elle a allégué que l'ancien camp aurait communiqué au nouveau camp des renseignements personnels sur son enfant sans son consentement. Parallèlement, elle a soutenu que le nouveau camp aurait recueilli, utilisé et communiqué à l'ancien camp des renseignements personnels sur son enfant sans son consentement.

Constatations

L'ancien camp nous a informés que le nouveau camp avait bel et bien communiqué avec lui pour obtenir des renseignements sur l'enfant et ses expériences antérieures à ce camp. L'ancien camp a reconnu qu'au cours de l'entretien les deux organisations ont échangé des renseignements sur l'enfant. Il a ajouté que ce type d'échange d'information informel est une pratique courante entre les camps.

Les renseignements partagés comprenaient l'historique récent des inscriptions et des expériences antérieures au camp de l'enfant; une opinion sur la personnalité de l'enfant et une évaluation du type de soutien requis par l'enfant dans le cadre d'un camp.

Nous avons été troublés d'apprendre que l'ancien camp n'avait pas de formulaire de consentement pour la communication de ce type de renseignements à des tiers. Nous avons également constaté que l'information sur la protection des renseignements personnels affichée sur le site Web de l'organisation était limitée et insuffisante pour l'obtention d'un consentement.

Pour ces raisons, nous avons conclu que l'ancien camp n'avait pas obtenu le consentement de la mère pour la communication des renseignements personnels de son enfant au nouveau camp.

Quant au formulaire de demande d'inscription (que la mère a signé) et aux politiques en matière de protection des renseignements personnels et de confidentialité du nouveau camp, aucun de ces documents ne mentionnait que le camp pouvait recueillir auprès de tierces parties des renseignements personnels sur les participants au camp.

Qui plus est, le libellé utilisé dans les documents du camp qui portaient sur la protection des renseignements personnels était trop vague pour permettre aux parents ou aux tuteurs de comprendre les buts précis pour lesquels les renseignements personnels recueillis sur les enfants seraient utilisés ou communiqués.

Par conséquent, nous avons conclu que le nouveau camp n'a pas obtenu le consentement de la mère pour la collecte, l'utilisation et la communication des renseignements personnels de son enfant.

Que s'est il passé ensuite?

Le Commissariat a publié un rapport d'enquête préliminaire à l'intention des deux camps. Ces échanges de renseignements informels étant réputés pratique courante, nous avons recommandé aux deux organisations d'obtenir le consentement pour toute communication de renseignements personnels, et de donner à leurs employés une formation sur leurs obligations en matière de protection de la vie privée.

Les deux camps se sont engagés à mettre en œuvre nos recommandations dans les délais prévus. Par conséquent, nous avons estimé que les plaintes étaient ***fondées et conditionnellement résolues***.

2.10 ENQUÊTE SUR UNE PLAINTE : *Un magasin cesse de capter, à l'aide d'une caméra, des images de la cour de son voisin*

Contexte

Après qu'un magasin de vente au détail ait subi un incendie et plusieurs autres problèmes de sécurité, le propriétaire a installé une caméra de surveillance vidéo extérieure à l'arrière du magasin. Outre le stationnement du magasin, l'appareil avait vue sur une voie publique et quelques maisons et propriétés commerciales tout près.

Le propriétaire de la maison située directement derrière le magasin s'est plaint de la caméra auprès du Commissariat. Il a allégué que celle ci captait, sans son consentement, des images de l'arrière de sa résidence, de son stationnement arrière, ainsi que de toute personne entrant dans sa maison ou en sortant.

Constatations

Le propriétaire du magasin nous a dit avoir besoin de la caméra pour se protéger contre le vol et le vandalisme. Il a donné une description détaillée des incidents de sécurité qui s'étaient produits au magasin au cours des dernières années et a déclaré qu'il n'avait pas les moyens de se payer les services d'un gardien de sécurité.

Aucun avis n'était affiché derrière le magasin pour alerter les personnes circulant sur la voie publique que la caméra était en opération. Des petits autocollants ont été apposés sur la porte arrière du magasin et sur la caméra, mais ils étaient illisibles de loin.

Le système d'enregistrement de la caméra fonctionnait en boucle, de sorte que les images étaient remplacées toutes les 72 heures. Les images enregistrées n'étaient archivées qu'en cas d'incidents de sécurité présumés.

À la lumière des antécédents du magasin en matière de sécurité, nous avons conclu qu'une caméra de sécurité était une mesure appropriée pour filmer la zone arrière du magasin.

Nous n'avons pas estimé, cependant, que la capture des images de la propriété du voisin constituait une fin appropriée pour la collecte de renseignements personnels. Par extension, ces images de surveillance ne devraient pas être captées sans le consentement des personnes concernées.

Que s'est il passé ensuite?

Lorsque nous avons expliqué au propriétaire du magasin les préoccupations relatives à la vie privée soulevées par son voisin, il a accepté de déplacer la caméra pour qu'elle cesse de capter des images de la résidence et de l'aire de stationnement du voisin.

Il a aussi affiché un avis approprié sur la porte arrière du magasin, informant les passants que la voie publique était sous surveillance vidéo et que leurs images seraient enregistrées. L'avis comprenait les coordonnées du magasin.

Nous avons estimé que ces mesures étaient suffisantes pour assurer la connaissance et le consentement implicites des personnes s'approchant de cette aire. Néanmoins, nous avons encouragé le propriétaire du magasin à limiter toute surveillance non nécessaire de la voie publique.

Nous avons conclu que la plainte était ***fondée et résolue***.

Lorsque le propriétaire du magasin nous a dit qu'il souhaitait se réserver le droit de remettre la caméra dans sa position initiale si les circonstances le dictaient, nous l'avons mis en garde encore une fois contre la capture d'images de l'entrée arrière de la résidence et de l'aire de stationnement du plaignant, au motif que cela contreviendrait à la LPRPDE. Nous lui avons fortement recommandé de lire et de suivre nos *Lignes directrices sur la surveillance vidéo au moyen d'appareils non dissimulés dans le secteur privé.*

2.11 ATTEINTE À LA PROTECTION DES DONNÉES

Le principe de responsabilité oblige les organisations confrontées à une atteinte à la protection des données à prendre toutes les mesures possibles pour en limiter l'incidence. À cette fin, elles doivent intervenir d'une manière rapide et globale pour mettre fin aux dommages, alerter les autorités, communiquer avec les personnes concernées et prêter assistance à celles ci.

Une fois la situation d'urgence passée, il faut aussi examiner les politiques et processus internes, et prendre toutes les mesures nécessaires pour assurer leur renforcement en cas d'incidents futurs.

Le Commissariat encourage les organisations à signaler volontairement les atteintes à la protection des données qui impliquent des renseignements personnels. Ces atteintes appartiennent à trois grands types :

La **communication accidentelle** se rapporte à des incidents où une organisation communique par accident des renseignements personnels à des personnes auxquelles ils ne sont pas destinés. Par exemple, des relevés de compte peuvent être envoyés à une mauvaise adresse à la suite d'une erreur mécanique ou humaine, ou des renseignements personnels sont rendus accessibles au public sur le site Web d'une organisation en raison d'un problème technique.

La **perte** se rapporte à des incidents où des renseignements personnels détenus par une organisation sont perdus, généralement à cause de la perte d'un ordinateur portatif, d'un CD ou de documents papier.

L'accès, l'utilisation ou la communication non autorisés comprennent tout incident dans lequel une personne ne disposant pas d'une autorisation de l'organisation accède aux renseignements personnels, les utilise ou les communique. Il peut s'agir, par exemple, du vol d'un ordinateur portatif, du piratage en ligne de la base de données d'une organisation, ou d'un employé qui accède à des renseignements personnels ou les utilise à des fins non autorisées.

En 2012, 33 atteintes à la protection des données dans le secteur privé nous ont été signalées volontairement. Il s'agit d'une diminution de près de 50 % par rapport aux 64 incidents signalés l'année précédente, et du nombre le plus faible d'atteintes signalées au Commissariat au cours des cinq dernières années.

Secteur	Communication accidentelle	Perte	Accès, utilisation ou communication non autorisés	Total	Proportion des atteintes par secteur
Secteur financier	4	2	13	19	58 %
Services			1	1	3 %
Assurances	2			2	6 %
Ventes/détail					
Télécommunications			3	3	9 %
Internet			1	1	3 %
Divertissement	1		2	3	9 %
Hébergement	1		1	2	6 %
Autre		1		1	3 %
Santé					
Services professionnels	1			1	3 %
Transports					
Total	9	3	21	33	
Proportion des atteintes par type	27 %	9 %	64 %	100 %	100 %

L'industrie financière est toujours le secteur qui nous signale régulièrement le plus grand nombre d'atteintes. L'année dernière, 19 atteintes ont été signalées pour ce secteur, soit une baisse de 34 % par rapport aux 29 incidents de l'année précédente.

Les signalements d'atteinte pour tous les autres secteurs se sont élevés à 14, passant ainsi d'un pic de 35 incidents enregistrés en 2011 à des niveaux comparables à ceux des autres années.

Le volume de signalements volontaires des atteintes que reçoit le Commissariat est évidemment influencé par le nombre d'atteintes qui se produisent dans les faits. Cependant, d'autres facteurs entrent également en jeu, notamment le niveau de sensibilisation dans les organisations quant au rôle du Commissariat dans la réception de ces signalements, et le choix des organisations de signaler ou non les incidents lorsqu'ils se produisent.

En raison de cette variabilité et des nombres relativement faibles qui sont concernés, nous ne pouvons pas expliquer la diminution des signalements observée en 2012 par rapport à l'année précédente. Toutefois, nous continuerons de surveiller les chiffres afin de déceler les tendances pertinentes.

Pour leur part, les responsables de la protection de la vie privée du secteur privé continuent d'affirmer qu'ils signalent proactivement les atteintes, même si une loi fédérale rendant obligatoires les signalements n'a pas encore été adoptée. Nous les félicitons de poursuivre ce travail d'une manière volontaire.

Après réception du signalement d'une atteinte, le Commissariat collabore avec le responsable de la protection de la vie privée de l'organisation pour veiller à ce que les mesures nécessaires soient prises afin d'atténuer les répercussions. Dans les cas où il est justifié d'aviser toutes les personnes concernées, nous nous efforçons de nous assurer qu'elles reçoivent des informations cohérentes, et que leurs préoccupations soient traitées de la manière la plus efficace et rapide possible.

Nous croyons qu'il est dans l'intérêt de tous d'endiguer les problèmes potentiels avant qu'ils ne dégénèrent en plaintes officielles auprès du Commissariat. Voici quelques exemples d'incidents liés à des atteintes qui nous ont signalés en 2012 :

2.11.1 *LinkedIn intervient promptement pour limiter les dommages à la suite d'une importante cyberattaque*

En juin 2012, LinkedIn, un site de réseautage d'affaires, s'est fait voler près de 6,5 millions de mots de passe d'utilisateurs qui ont été affichés en ligne. Bien que l'atteinte ait mis en lumière des faiblesses dans ses mesures de protection des renseignements, LinkedIn est néanmoins intervenu rapidement à l'égard de l'atteinte et a coopéré avec le Commissariat et ses homologues de la Colombie-Britannique, de l'Alberta et du Québec.

L'engagement du site en vue de la résolution de la situation émanait clairement du sommet, la haute direction ayant autorisé un « code rouge » d'intervention, de manière à accorder à l'atteinte le plus haut degré de priorité au sein de l'organisation et à déclencher un déploiement immédiat de ressources pour y faire face.

LinkedIn a ensuite assuré le suivi au moyen de l'examen de son intervention, de l'évaluation des leçons retenues par l'organisation et du renforcement supplémentaire de ses mesures de protection des renseignements.

LinkedIn, comme beaucoup d'organisations, aurait pu s'être dotée de mesures plus efficaces de protection des renseignements. Cela dit, après avoir examiné sa réaction lorsqu'elle a été confrontée à une cyberattaque, nous avons conclu qu'elle avait fait preuve d'une diligence raisonnable et s'était montrée responsable.

2.11.2 *Un employé d'une entreprise de services de placements répond à un courriel « hameçon »*

Un employé d'une entreprise de services de placements a répondu à un courriel « hameçon » qui semblait provenir d'une grande banque. Le courriel frauduleux demandait la confirmation d'un code d'utilisateur et d'un mot de passe. Les renseignements ont ensuite été utilisés pour accéder à des comptes d'entreprise et consulter les renseignements bancaires d'un petit nombre de clients.

L'entreprise de services de placements a immédiatement désactivé le code d'utilisateur et le mot de passe compromis, et a informé le service de police local, le Groupe des enquêtes sur les fraudes de la Gendarmerie royale du Canada et le Commissariat.

Les clients concernés ont été avisés de l'atteinte et on leur a recommandé de surveiller les transactions effectuées dans leur compte. À titre de précaution supplémentaire, on leur a aussi conseillé de communiquer avec les deux principaux bureaux de crédit pour qu'une alerte à la fraude soit inscrite dans leur dossier.

2.11.3 *Un ordinateur portatif est volé en même temps que des renseignements concernant le mot de passe*

Un conseiller financier travaillant à titre d'entrepreneur indépendant pour une entreprise de services financiers s'est fait voler un ordinateur portatif, une clé USB et un agenda qui se trouvaient dans une voiture verrouillée. Le matériel volé comprenait des renseignements personnels et financiers délicats au sujet de 188 clients.

L'ordinateur était protégé par un mot de passe et les données qu'il contenait étaient chiffrées, mais le mot de passe et des renseignements sur le logiciel de cryptage étaient notés dans l'agenda.

L'entreprise a informé le service de police local, ainsi que le Commissariat. L'entreprise a également communiqué avec tous les clients concernés et leur a offert des services gratuits de surveillance du crédit.

2.12 MISE À JOUR DE LA POLITIQUE DE CONFIDENTIALITÉ DE GOOGLE : *Des préoccupations demeurent en ce qui concerne le regroupement des données et leur conservation*

L'année dernière, au mois de mars, Google a mis en place une nouvelle politique de confidentialité. L'entreprise ayant fait l'acquisition de nombreux autres produits et services, tous assortis de leurs propres politiques de confidentialité, elle a décidé de rassembler toutes les politiques en une seule politique de confidentialité concise et plus facile à lire.

Cette intégration des multiples politiques existantes en une seule s'inscrivait dans le cadre des efforts déployés par Google afin de simplifier les services offerts aux détenteurs d'un compte Google. Ainsi, lorsque l'utilisateur ouvre une session dans son compte, Google réunit les données qu'il a fournies pour un service et celles qu'il a fournies pour d'autres services.

Du point de vue de Google, cette approche permet une « expérience Google plus conviviale et intuitive » [traduction]. En combinant les données de cette façon, Google se proposait aussi d'améliorer les résultats de recherche et de rendre les publicités plus pertinentes pour les utilisateurs.

Nous avons examiné l'incidence sur la vie privée des changements apportés à la politique de confidentialité de Google, en mettant l'accent sur le manque de précisions au sujet de la conservation des données, sur les conséquences de l'établissement de liens entre les renseignements personnels fournis par les détenteurs d'un compte pour profiter de différents services, et sur les répercussions de cette approche sur les utilisateurs d'appareils mobiles qui utilisent le système d'exploitation Android de Google.

Nous avons demandé à Google d'inclure dans sa politique de confidentialité plus de renseignements sur ses pratiques de conservation des données. Nous lui avons aussi demandé de mieux informer les détenteurs d'un compte de l'établissement de liens entre leurs renseignements personnels et de la procédure à suivre pour se soustraire à cette pratique.

Nous n'étions pas la seule autorité de protection des données à faire part de nos préoccupations à Google. Les autorités de protection de la vie privée de la zone Asie Pacifique (un groupe auquel nous participons), ainsi que la Commission nationale de l'informatique et des libertés (CNIL), au nom du Groupe de travail Article 29, ont également écrit à Google pour lui conseiller d'apporter certaines modifications. La CNIL a réalisé, pour le compte du Groupe de travail Article 29 un examen très approfondi de la nouvelle politique et a formulé des recommandations précises à l'entreprise.

Au moment de rédiger ce rapport, Google n'avait pas changé sa politique de confidentialité, ou indiqué si elle le ferait.

2.13 MISE À JOUR D'UNE VÉRIFICATION DE LA CONFORMITÉ : *Une autorité indépendante confirme que Bureau en Gros a répondu aux préoccupations relatives à la protection de la vie privée*

En juin 2011, le Commissariat a publié le rapport d'une vérification de la conformité qu'il avait réalisée au sujet des pratiques de gestion des renseignements personnels de Bureau en Gros.

La vérification a été réalisée à la suite d'enquêtes précédentes sur des plaintes liées à des dispositifs électroniques qui avaient été achetés, utilisés et retournés au magasin, et ensuite revendus, alors qu'ils contenaient encore les renseignements personnels de l'acheteur précédent. Le Commissariat a confirmé que divers dispositifs de stockage de données étaient revendus sans que toutes les données résiduelles aient été entièrement effacées, entraînant ainsi une communication inappropriée de renseignements personnels.

La vérification exhaustive que nous avons réalisée par la suite a donné lieu à l'élaboration de dix recommandations que Bureau en Gros a accepté d'appliquer. En voici quelques unes :

- Revoir les procédures et processus relatifs à la suppression des renseignements enregistrés sur les dispositifs de stockage de données et mettre en place des mesures de vérification renforcées afin d'éliminer toute possibilité que des renseignements personnels soient communiqués à des tiers;
- Limiter la période de conservation des renseignements personnels associés aux demandes d'impression et de copie en ligne;
- S'assurer que les renseignements personnels sont conservés dans des classeurs verrouillés ou des zones sécurisées;
- Prévoir la réalisation d'examens de la conformité en matière de protection de la vie privée dans le cadre du programme de vérification interne;
- Assigner aux employés des codes d'accès uniques au système.

Lorsque le rapport de la vérification a été rendu public, la commissaire a demandé que Bureau en Gros engage une société d'experts conseils indépendante pour confirmer que l'entreprise a bien mis en œuvre toutes les mesures nécessaires pour donner suite aux recommandations.

Que s'est il passé ensuite?

Bureau en Gros a fait appel aux services d'une société d'experts conseils indépendante, qui a attesté que l'entreprise avait pris les mesures nécessaires pour donner suite à nos recommandations et que de nouvelles procédures étaient en place. La vérification indépendante a notamment confirmé que Bureau en Gros avait mis en œuvre un processus pour supprimer les données des clients qui étaient enregistrées sur les produits retournés.

La société d'experts conseils qui a effectué la vérification s'est dite convaincue que la nouvelle procédure permettrait de faire en sorte que toutes les données appartenant à des clients et contenues sur des dispositifs de stockage de données soient effacées avant que les dispositifs soient remis en vente.

Répondre à vos préoccupations en matière de protection de la vie privée

En 2012, nous avons poursuivi notre travail pour aider des Canadiennes et Canadiens perplexes devant les nouvelles technologies de l'information, préoccupés par leurs droits en vertu des lois relatives à la protection de la vie privée ou irrités par le traitement réservé à leurs renseignements personnels par des entreprises privées.

Les préoccupations de la population canadienne en ce qui a trait à la protection de la vie privée ont donné lieu à des milliers de demandes de renseignements et à des centaines de plaintes déposées auprès du Commissariat. Comme toujours, nous avons tout mis en œuvre pour répondre à ces préoccupations de façon attentionnée et avec respect, et pour proposer des solutions appropriées et opportunes.

Ce chapitre présente le travail réalisé en 2012 par notre Centre d'information et nos équipes d'enquête sur des questions liées à la LPRPDE. Il met l'accent sur nos efforts constants pour simplifier et améliorer nos processus, pour le bénéfice à la fois des plaignants et des mis en cause.

Le Commissariat s'est également consacré à l'avancement des connaissances dans le domaine de la protection de la vie privée. Ce chapitre met en relief notre Programme des contributions pour le financement de la recherche, qui a été remanié en 2012 grâce à un nouveau plan stratégique quinquennal, ainsi que d'autres travaux que nous avons effectués ou commandés dans des domaines aussi divers que les fuites sur Internet, l'analyse prédictive et les tests génétiques offerts en ligne directement aux consommateurs.

Nous présentons également dans ce chapitre un sommaire des observations clés que nous avons recueillies auprès des entreprises dans le cadre de notre sondage biennal sur les attitudes et pratiques en matière de protection des renseignements personnels des entreprises canadiennes. Puisque le maintien d'un dialogue avec les intervenants est une priorité pour

nous, ce chapitre fait également le point sur le vaste éventail d'initiatives de sensibilisation entreprises par le Commissariat, tant à Ottawa qu'à Toronto.

Les connaissances que nous acquérons par ces divers moyens influent sur notre travail d'une multitude de façons. Elles garantissent notamment que les documents d'orientation, les politiques et autres outils que nous élaborons sont concrets, à jour et répondent aux besoins du public cible. Outre les nouvelles lignes directrices en matière de responsabilité décrites au chapitre 2, d'autres documents que nous avons publiés en 2012 ont traité de sujets spécialisés comme l'infonuagique, la publicité comportementale en ligne et les applications mobiles.

Comme l'explique le présent chapitre, notre objectif est de renforcer le respect volontaire de la LPRPDE par les organisations. Au fil des ans, nous espérons que cela se traduira par une diminution des problèmes liés à la protection de la vie privée pour la population canadienne.

3.1 CENTRE D'INFORMATION

Notre Centre d'information a reçu 4 474 demandes de renseignements sur des questions liées à la protection de la vie privée dans le secteur privé en 2012. Environ neuf demandes sur dix ont été faites par téléphone, comme par les années passées.

Le secteur des télécommunications a fait l'objet de 14 % des demandes de renseignements, ce qui en fait le secteur le plus souvent visé par des demandes de renseignements. Il a été suivi de près par le secteur bancaire (13,5 % de toutes les demandes de renseignements). Nous avons aussi reçu un nombre important de demandes de renseignements liées au secteur de l'hébergement, représentant 5 % du total des demandes.

Pour ce qui est du contenu des demandes, les Canadiennes et Canadiens ont surtout été préoccupés par la communication possible de leurs renseignements personnels sans leur consentement et par le traitement de leur identité et de leurs renseignements personnels par les organisations. On a observé une hausse du nombre d'appels chaque fois qu'une atteinte à la protection des données a été largement médiatisée.

Comme chaque année, le Commissariat a continué de recevoir beaucoup d'appels au sujet de la collecte de renseignements personnels de nature délicate, notamment le numéro d'assurance sociale. Les appelants ont aussi cherché à se renseigner sur la marche à suivre pour accéder à leurs renseignements personnels détenus par des entreprises.

De plus, nous avons reçu de nombreuses demandes d'information sur la procédure du Commissariat relativement au dépôt de plaintes ayant trait à la protection de la vie privée.

3.2 RÉCEPTION DES PLAINTES

La Direction des enquêtes liées à la LPRPDE du Commissariat a continué en 2012 de chercher des moyens efficaces de répondre aux préoccupations de la population canadienne relativement à la protection de la vie privée.

C'est ainsi qu'au cours de l'été, nous avons facilité l'accès au Commissariat par voie électronique afin d'aider les Canadiennes et Canadiens à faire respecter plus efficacement leur droit à la vie privée. Nous avons mis en place un formulaire de plainte en ligne qui permet aux gens d'exprimer leurs inquiétudes, de joindre des documents à l'appui et de soumettre leurs plaintes par l'entremise de notre portail en ligne sécurisé, éliminant ainsi la nécessité d'imprimer et d'envoyer les documents par courrier ou télécopieur.

Nous avons également tâché de résoudre plus de dossiers dans un délai raisonnable et d'une manière satisfaisante tant pour les plaignants que pour les organisations mises en cause. Les retards sont regrettables pour tous et peuvent entraîner pour le Commissariat une surcharge de travail en raison du nombre important de dossiers en retard.

Nous avons, à cette fin, continué de veiller à optimiser l'éventail des moyens à notre disposition pour traiter les plaintes. Notre unité de la réception des plaintes a joué un rôle de premier plan dans l'assignation appropriée des dossiers, qu'il s'agisse de les acheminer aux agents de règlement rapide, au processus d'enquête officielle du Commissariat ou à d'autres organismes mieux à même de traiter le différend.

Nous avons également poursuivi des négociations en vue du règlement de certains enjeux et, dans certains cas, nous avons eu recours au pouvoir discrétionnaire de la commissaire pour refuser de mener une enquête ou y mettre fin.

Dans l'ensemble, nous avons tenté de nous en tenir aux questions importantes — à savoir les plaintes relatives à des problèmes sérieux et systémiques qui présentent les plus importants risques d'atteinte à la vie privée pour la population canadienne.

Ces initiatives ont notamment permis d'enregistrer une augmentation de 21 % du nombre d'enquêtes officielles menées par rapport à l'année précédente; le nombre s'est établi à 145 pour 2012, soit un résultat dont nous sommes particulièrement satisfaits.

3.2.1 *Observations écrites reçues*

Toutes les observations écrites reçues au sujet d'enjeux ayant trait à la protection de la vie privée, à l'exception de celles formulées contre des institutions fédérales, sont transmises à l'unité de la réception des plaintes liées à la LPRPDE à des fins de tri initial. En 2012, nous avons reçu 705 plaintes écrites de cette nature, soit un nombre comparable à celui des dernières années.

L'unité passe en revue les observations et, lorsqu'il y a lieu, assure un suivi auprès du plaignant pour obtenir des précisions et réunir d'autres renseignements ou documents nécessaires.

Si le plaignant n'a pas déjà discuté du problème avec le responsable de la protection de la vie privée de l'organisation concernée, un agent de l'unité de la réception des plaintes lui demandera d'essayer de résoudre directement la question avec l'organisation, et de communiquer de nouveau avec le Commissariat en cas d'échec.

Un plaignant sur quatre a ainsi été redirigé vers le responsable de la protection de la vie privée de l'organisation concernée en vue de régler rapidement et directement le problème.

Les agents de l'unité de la réception des plaintes sont souvent en mesure de régler immédiatement les différends, éliminant ainsi la nécessité de recourir à une plainte officielle.

Par exemple, nous pouvons informer un plaignant qu'une enquête précédente a révélé que les activités faisant l'objet de la plainte sont en fait autorisées en vertu de la LPRPDE. De même, si nous avons déterminé auparavant que nous n'avons pas compétence sur l'organisation ou le type d'activité en question, nos agents essaient de rediriger la personne vers d'autres ressources ou services d'assistance.

Un tiers des plaintes n'ont pas été acceptées parce que rien n'indiquait qu'il y avait eu atteinte en vertu de la LPRPDE, ou parce qu'elles portaient sur une question pour laquelle le Commissariat n'a pas compétence. D'autres n'ont pas été acceptées faute de renseignements suffisants pour mener l'enquête, ou parce que le problème a été réglé de manière satisfaisante au cours du processus de réception.

3.2.2 *Plaintes acceptées, par secteur d'activité*

En fin de compte, nous avons accepté 220 plaintes en 2012, lesquelles ont par la suite été dirigées vers notre processus de règlement rapide ou celui des enquêtes officielles.

Près d'une plainte sur quatre visait le secteur financier, qui comprend les banques, les sociétés émettrices de cartes de crédit, les courtiers hypothécaires, les conseillers financiers et les entreprises connexes. Cette tendance est observée chaque année, fort probablement en raison de la taille et de la portée du secteur et du nombre gigantesque de transactions effectuées.

Selon notre expérience, les institutions financières sont parmi les organisations du secteur privé qui élaborent certaines des meilleures politiques et pratiques en matière de protection de la vie privée. Néanmoins, des améliorations peuvent encore être apportées, en particulier en ce qui a trait à l'application uniforme des politiques et des pratiques en matière de collecte, à la formation des employés et aux mesures de protection des renseignements personnels.

Les secteurs des services de télécommunications et d'Internet occupaient tous deux le deuxième rang des secteurs visés par le plus grand nombre de plaintes — c'est-à-dire que chacun a été visé par environ la moitié des plaintes acceptées pour le secteur financier. Cette tendance reflète l'importance grandissante de l'économie numérique, de même que les risques relatifs à la protection de la vie privée qui sont

inhérents au fait d'utiliser et d'échanger une quantité aussi importante de renseignements personnels.

La plupart des plaintes liées aux télécommunications portaient sur l'accès à l'information liée aux comptes. Les plaintes concernant Internet étaient plus diversifiées et comprenaient notamment des problèmes de consentement et d'utilisation de l'information affichée.

Secteur d'activité ayant enregistré le plus grand nombre de plaintes, en pourcentage de toutes les plaintes acceptées*

Secteur	2012	2011	2010
Secteur financier	22	22	22
Télécommunications	11	11	9
Services Internet	11	6	9
Services	10	10	17
Assurance	7	9	13

* Vous trouverez des statistiques et des définitions pour tous les secteurs d'activité à l'annexe 2.

3.2.3 *Types de plaintes acceptées*

Les trois principaux types de plaintes acceptées l'an dernier en vertu de la LPRPDE se rapportaient à ce qui suit :

- difficultés d'accéder à ses renseignements personnels;
- utilisation et communication inappropriées de renseignements personnels;
- collecte excessive de renseignements personnels.

Ces résultats ont été comparables à ceux des autres années, à ceci près que les plaintes relatives aux demandes d'accès ont dépassé celles sur l'utilisation et la communication de renseignements personnels au titre de principale source de préoccupation.

Les plaintes relatives à l'accès peuvent porter sur un refus total ou partiel de donner accès aux renseignements personnels demandés, sur des retards indus dans la réception des renseignements demandés ou sur des désaccords quant à la définition de ce qui constitue des renseignements personnels devant être fournis par les entreprises en vertu de la LPRPDE.

Type de plaintes le plus courant, en pourcentage de toutes les plaintes acceptées

	2012	2011	2010
Accès: Plaintes concernant la difficulté d'accéder à ses renseignements personnels.	30	26	24
Utilisation et communication: Plaintes concernant l'utilisation ou la communication inappropriées de renseignements personnels, sans consentement de l'intéressé, à des fins autres que celles pour lesquelles ils ont été recueillis.	26	32	27
Collecte: Plaintes concernant la collecte non nécessaire de renseignements personnels ou la collecte trompeuse ou illégale, par exemple sans le consentement adéquat de l'intéressé.	15	20	16

3.3 RÈGLEMENT RAPIDE DES PLAINTES

Lorsque nous acceptons une plainte écrite qui semble pouvoir faire l'objet d'un règlement rapide, l'unité de la réception des plaintes transmet le dossier à un agent de règlement rapide. Celui ci collabore avec le plaignant et l'organisation mise en cause pour résoudre la plainte dans un esprit de concertation et souvent de conciliation.

Des problèmes qui peuvent prendre des mois à résoudre dans le cadre d'une enquête officielle sont susceptibles d'être réglés en quelques jours grâce à notre processus de règlement rapide. Ce mécanisme a été acclamé ces dernières années tant par les plaignants que les organisations mises en cause.

En 2012, nous avons tenté de régler rapidement 138 plaintes, ce qui représente une hausse de 10 % par rapport à l'année précédente. Nous avons été en mesure d'atteindre un règlement satisfaisant dans 115 de ces cas, soit 83 %. Les 23 cas restants ont été réassignés pour enquête officielle.[2]

Cas acceptés pour règlement rapide	Cas réglés à l'aide du règlement rapide	Cas renvoyés pour enquête plus approfondie
138	115	23

En moyenne, les plaintes traitées à l'aide de ce processus ont été réglées 2,8 mois après la date de leur acceptation. Bien que cela représente une légère hausse par rapport au délai moyen de traitement de 2 mois enregistré l'année précédente, ce type de règlement demeure néanmoins une option beaucoup plus rapide que l'enquête officielle.

Voici quelques exemples de cas qui ont été réglés avec succès dans le cadre du processus de règlement rapide.

[2] Vous trouverez des statistiques détaillées sur le secteur, le type et les interventions en matière de règlement rapide à l'annexe 2

3.3.1 *Une entreprise de services publics cesse de recueillir certains renseignements personnels*

Une personne, ayant fait une demande en ligne pour devenir cliente d'une entreprise de services publics, s'est inquiétée de voir des champs obligatoires exigeant des demandeurs qu'ils fournissent leurs numéros d'assurance sociale et de permis de conduire, ainsi que des renseignements sur leur employeur.

Lorsque l'entreprise a été interrogée à ce sujet, elle a indiqué que cette information était nécessaire pour authentifier les clients qui communiquent avec elle. La personne n'était pas satisfaite de la réponse et a déposé une plainte auprès du Commissariat.

L'agent de règlement rapide a communiqué avec l'entreprise pour l'informer de l'éventail restreint de circonstances pour lesquelles les numéros d'assurance sociale et les numéros de permis de conduire peuvent être recueillis, ainsi que des risques liés au fait de recueillir trop de renseignements sur les employeurs. L'agent a également transmis à l'entreprise de services publics plusieurs de nos documents d'orientation.

En guise de réponse, l'entreprise a cessé de recueillir les numéros de permis de conduire et les numéros d'assurance sociale, et ne rend plus obligatoires les renseignements sur l'employeur. Elle a remplacé cette information par des questions de sécurité visant à authentifier les titulaires de compte.

L'entreprise s'est montrée reconnaissante de l'information que nous avons fournie, et la plaignante a été satisfaite des mesures prises par l'entreprise.

3.3.2 *Un détaillant étranger remplace le NAS par un NIP*

Une cliente d'un commerce de détail de vente directe a dû fournir son numéro d'assurance sociale pour bénéficier d'une réduction sur un achat. Lorsque l'entreprise a été interrogée à ce sujet, elle a expliqué qu'elle utilisait les quatre derniers chiffres du numéro pour authentifier ses « clients privilégiés ».

Avant de porter plainte auprès du Commissariat, la cliente a consulté les lignes directrices affichées sur notre site Web relativement à l'utilisation appropriée du numéro d'assurance sociale. Elle a aussi communiqué avec notre Centre d'information pour confirmer la validité de sa plainte en vertu de la LPRPDE.

Notre agent de règlement rapide a communiqué avec l'entreprise, située à l'extérieur du Canada, pour l'informer que le fait d'exiger des clients qu'ils fournissent leur numéro d'assurance sociale dans ce contexte et de l'utiliser à titre d'identificateur n'étaient pas des pratiques raisonnables en vertu de la LPRPDE.

L'agent a souligné la nature délicate de ce numéro et la façon dont sa collecte investissait l'entreprise d'une responsabilité potentielle en cas d'atteinte à la protection des données.

En guise de réponse, l'entreprise s'est engagée à revoir la formation du personnel de son centre d'appel et du service des ventes pour qu'il ne demande plus les numéros d'assurance sociale. Les employés

proposeront plutôt aux clients de choisir un numéro d'identification personnel de quatre chiffres, ou NIP.

L'organisation a ajouté qu'elle modifierait ses formulaires de façon à supprimer toute référence au numéro d'assurance sociale (ou à son équivalent dans d'autres pays).

L'entreprise a réagi rapidement et a apporté des correctifs importants pour se conformer à la LPRPDE. La plaignante a été satisfaite de ces mesures.

3.3.3 *Une compagnie d'assurances supprime des dossiers archivés pour se conformer aux règles de conservation*

Un plaignant a communiqué avec une compagnie d'assurances pour obtenir une soumission d'assurance. Ce faisant, le plaignant a appris que la compagnie détenait toujours dans ses archives un dossier de soumission qui lui avait été transmis cinq ans plus tôt.

Le plaignant, qui n'était pas client de cette compagnie d'assurances, s'est opposé à ce que l'organisation conserve des renseignements le concernant et a demandé que la soumission initiale soit effacée. La compagnie a refusé.

Après que la personne ait formulé une plainte auprès du Commissariat, notre agent de règlement rapide a informé la compagnie d'assurances que les renseignements personnels ne peuvent être conservés qu'aussi longtemps qu'ils sont nécessaires aux fins pour lesquelles le consentement de la personne a été obtenu initialement.

En guise de réponse, la compagnie a lancé un vaste programme pour mettre fin à la conservation excessive des renseignements personnels dans ses bases de données, y compris des soumissions initiales de polices, et rendre les pratiques conformes à la LPRPDE.

Le plaignant a été satisfait de la réponse.

3.3.4 *Une entreprise propose à ses employés une nouvelle formation sur le traitement des demandes liées à la protection de la vie privée*

Un client, qui avait certaines inquiétudes au sujet des pratiques en matière de protection de la vie privée du sous traitant d'un grand détaillant, a eu beaucoup de mal à déterminer le mécanisme de recours approprié pour faire part de ses préoccupations.

Les employés à qui il a parlé ne connaissaient pas bien les obligations de l'entreprise en matière de protection de la vie privée en vertu de la LPRPDE et étaient incapables de le diriger vers le responsable de la protection de la vie privée de l'organisation, comme l'exige le principe de responsabilité énoncé dans la LPRPDE.

Lorsque notre agent de règlement rapide a communiqué avec l'entreprise, cette dernière s'est dite surprise d'apprendre qu'en dépit de ses nombreuses tentatives, le client n'avait jamais été dirigé vers la personne directement responsable des questions liées à la protection de la vie privée.

L'entreprise a promis d'offrir une formation obligatoire à son personnel pour améliorer la capacité

des employés à gérer les plaintes liées à la protection de la vie privée et notamment à diriger les personnes vers les autorités compétentes.

Le plaignant a été satisfait de cet engagement.

3.4 SERVIR LA POPULATION CANADIENNE AU MOYEN D'ENQUÊTES SUR LES PLAINTES

Toutes les plaintes ne se prêtent pas à un règlement rapide. Celles qui soulèvent des questions complexes ou systémiques ou qui renvoient à des enjeux nouveaux continuent d'être traitées dans le cadre du processus d'enquête officielle.

En 2012, nous avons réalisé 145 enquêtes sur des plaintes en vertu de la LPRPDE, soit 21 % de plus que l'année précédente. Dans la plupart des cas (140 sur 145), nous avons été en mesure de trouver un règlement satisfaisant aux questions soulevées. Seules cinq enquêtes ont donné lieu à des plaintes jugées « fondées », ce qui signifie que nous n'avons pu parvenir à aucun règlement acceptable.

Enquêtes réalisées	Enquêtes conclues avec un règlement satisfaisant	Plaintes jugées fondées; cas restés non résolus
145	140	5

En dépit de la hausse marquée du nombre de plaintes acceptées pour enquête officielle, la durée moyenne des enquêtes a diminué pour atteindre 12,6 mois en 2012, ce qui représente une baisse de 12 % par rapport au délai de 14,3 mois relevé l'année précédente.

Si l'on tient compte des plaintes résolues au moyen du processus de règlement rapide, le délai moyen de traitement des dossiers s'établissait à 8,3 mois en 2012, c'est-à-dire qu'il était presque identique à celui de l'année précédente, et qu'il se situait bien en deçà des 12 mois exigés en vertu de la LPRPDE.

Nous avons été satisfaits de constater que, même si nous avons enquêté sur un plus grand nombre de cas et amélioré nos délais de traitement, nous sommes parvenus en même temps à réduire le nombre de nos dossiers en attente. Vers la fin de l'année, nous avions 141 plaintes toujours actives en examen, soit un recul de 20 % par rapport aux 177 dossiers restés actifs à la fin de 2011.

Ces tendances encourageantes sont dues, au moins en partie, au succès continu de nos efforts de règlement rapide. Sur le nombre total de 260 plaintes que nous avons traitées en 2012, 115, soit 44 %, ont été réglées à l'aide de stratégies de règlement rapide.

Des statistiques supplémentaires sur le secteur, le type et les décisions concernant les enquêtes terminées figurent à l'annexe 2. Les résumés de nombreux cas sur lesquels nous avons enquêté sont présentés aux chapitres 1 et 2.

3.5 AVANCEMENT DES CONNAISSANCES

3.5.1 *Programme des contributions*

Nous avons lancé, en 2012, notre dixième appel annuel de propositions dans le cadre du Programme des contributions du Commissariat, considéré comme l'un des plus importants programmes de recherche sur la protection de la vie privée. Nous avons également élaboré une nouvelle stratégie en six points pour renforcer l'influence du programme dans le domaine du droit à la vie privée au Canada.

Le programme, dont le mandat est défini en vertu de la LPRPDE, finance des projets de recherche indépendants sur la protection de la vie privée et des initiatives connexes de transfert des connaissances.

Voici quelques uns des projets que nous avons financés en 2012 :

- une étude des nouveaux défis en matière de protection de la vie privée liés aux innovations dans la recherche sur la thérapie cellulaire;
- une analyse de l'étendue de la communication volontaire d'information par les entreprises du secteur privé aux forces de l'ordre dans le cadre d'enquêtes sur la cybercriminalité;
- l'élaboration d'une série de reportages de fond et d'autres outils d'information pour la radio et les sites Web francophones qui fournissent de l'information pratique sur la protection des renseignements personnels;
- un outil de mise en correspondance interactif pour aider les Canadiennes et Canadiens à mieux comprendre l'infonuagique et son incidence sur leurs renseignements personnels;
- une enquête sur les applications pour téléphones intelligents et les risques associés à la protection de la vie privée pour les utilisateurs finaux;

Le Programme des contributions encourage les chercheurs à proposer des projets qui donneront naissance à de nouvelles idées et connaissances en matière de protection de la vie privée que les organisations pourront utiliser pour mieux protéger les renseignements personnels ou que les Canadiennes et Canadiens pourront utiliser pour prendre des décisions plus éclairées en ce qui a trait à la protection de leur vie privée.

Un appel de propositions est lancé chaque année à l'automne. Les établissements universitaires et les organismes sans but lucratif sont admissibles à obtenir un financement. Les projets sont choisis au terme d'un processus concurrentiel, et le travail de recherche qui s'ensuit est mené d'une manière indépendante du Commissariat.

Depuis sa conception en vertu de la LPRPDE et son lancement subséquent en 2004, le programme a versé environ 3 millions de dollars à près de 90 initiatives. Le budget annuel du programme s'élève à 500 000 $, et le montant maximal pouvant être accordé à tout projet est de 50 000 $.

- un rapport sur les répercussions de l'utilisation des technologies de l'information sur la protection de la vie privée dans des situations de violence familiale, de violence sexuelle et de harcèlement.

Nouvelle stratégie

Afin d'accroître les retombées du programme auprès des intervenants et au Canada en général, nous avons adopté une nouvelle stratégie quinquennale en 2012. Cette stratégie est fondée sur six points :

- **Accroître la portée du programme au moyen de partenariats**
  Nous avons exploré des possibilités de partenariat avec d'autres organismes fédéraux de financement. En premier lieu, nous avons établi un dialogue avec le Conseil de recherches en sciences humaines et Industrie Canada en tant que collaborateurs dans l'organisation du symposium de recherche *Parcours de protection de la vie privée*. (Voir l'encadré pour de plus amples renseignements.)

- **Permettre le transfert et la mise en application des connaissances**
  Nous avons révisé notre appel de propositions pour encourager les candidats qui souhaitent réaliser des projets de recherche à y intégrer des plans de transfert des connaissances. L'objectif est de faciliter la mise en application des résultats de recherche par les utilisateurs finaux. La série de symposiums de recherche *Parcours de protection de la vie privée* et certains documents connexes qui seront publiés en 2013 visent à présenter les retombées réelles des projets que nous avons financés sur la vie des Canadiennes et Canadiens.

- **Améliorer l'évaluation par des pairs**
  Nous avons mis sur pied, en 2012 et pour la toute première fois, un groupe d'examinateurs externes dont les membres sont issus des universités, de la société civile et du gouvernement, afin d'élargir l'expertise appliquée au processus d'évaluation du programme. L'expertise des examinateurs externes complémente l'expertise des intervenants à l'interne. Les examinateurs externes constituent en outre d'excellents ambassadeurs pour le programme.

- **Simplifier l'accessibilité au moyen d'améliorations techniques**
  Nous avons revu la section du site Web du Commissariat qui porte sur le Programme des contributions afin de faciliter la recherche et la consultation des projets financés par les utilisateurs finaux et les intervenants concernés.

- **Évaluer le succès du programme**
  Nous avons mené une étude bibliométrique des produits livrables du programme au fils des ans pour déterminer dans quelle mesure les résultats des projets de recherche ont été repris par la

communauté dans les revues spécialisées, les articles, les sites Web et sur les médias sociaux.

- **Renouveler notre stratégie de communication avec le public**
  Une nouvelle stratégie de communication proactive a été élaborée et fait l'objet d'une mise en œuvre afin de mieux promouvoir les possibilités de financement offertes en vertu du programme et de présenter les résultats réels des projets financés. L'amélioration de la communication permettra également de mieux faire connaître le programme aux candidats potentiels, de manière à continuer de recevoir des propositions de projets de recherche de haute qualité.

Symposium de recherche et formation interne

Le 2 mai 2012, le Commissariat tenait son premier symposium de recherche *Parcours de protection de la vie privée* à Ottawa. La série de symposiums vise à mettre en valeur les projets de recherche portant sur la protection de la vie privée financés par notre Programme des contributions et les organisations partenaires. Elle a également pour but de faciliter le dialogue entre les chercheurs et les personnes dont la vie et les entreprises sont concernées par les résultats de la recherche.

Le thème du premier symposium était « La protection de la vie privée pour tous » et les sous thèmes concernaient notamment la transformation du contexte relatif à la vie privée pour les jeunes, les moyens de joindre divers groupes, les différents points de vue culturels liés à la protection de la vie privée et les limites de l'identification et de la surveillance parmi différents groupes.

Plus de 130 participants issus notamment des universités, du gouvernement, d'organisations sans but lucratif et d'organismes de réglementation de la protection de la vie privée ont assisté à cet événement d'une journée, organisé avec l'aide du Conseil de recherches en sciences humaines et Industrie Canada.

Entre temps, nous avons également mis au point une série de conférences internes intitulée Conversations sur la protection de la vie privée pour promouvoir le dialogue et l'échange de connaissances à l'échelle de notre propre organisation.

Nous avons eu droit à une vue d'ensemble de la jurisprudence récente en matière de protection de la vie privée, ainsi qu'à des présentations sur l'analyse prédictive, les applications mobiles et les derniers résultats des projets de recherche financés dans le cadre de notre Programme des contributions.

3.5.2 *Recherche concernant les fuites sur Internet*

Les « fuites sur Internet » désignent la communication des renseignements personnels d'un utilisateur d'un site Web à des sites tiers, à l'insu ou sans le consentement de ce l'intéressé. Les sites Web qui ne prennent pas soin de limiter la divulgation peuvent ainsi communiquer un vaste éventail de renseignements personnels, comme des noms, des adresses de courriel et d'autres données, à des tiers.

Les fuites sur Internet étant devenues une source de préoccupations grandissante à l'échelle internationale,[1] le Commissariat a entrepris en 2012 des recherches pour déterminer si les sites Web canadiens divulguaient aussi les renseignements personnels des utilisateurs à des tiers. Nous avons publié nos conclusions en septembre, lesquelles indiquaient que plusieurs sites populaires auprès des Canadiennes et Canadiens ont effectivement communiqué des données personnelles, parfois dans une mesure importante.

Le contexte technique

Lorsqu'une personne consulte le site Web d'une organisation donnée, le contenu du site peut provenir de différentes sources extérieures à cette organisation. Par exemple, un site Web peut tirer des revenus en autorisant des organisations tierces à passer des annonces publicitaires sur son site, ou confier certaines fonctions à des tiers fournisseurs de services.

Dans le cas des publicités d'un tiers, lorsqu'un utilisateur télécharge une page sur un site Web participant, le gestionnaire du site Web envoie une requête à un annonceur pour lui demander d'afficher une annonce sur la page Web. C'est durant ce processus d'« appel de publicité » que le site Web peut révéler les renseignements personnels de l'utilisateur à un tiers, comme l'annonceur.

De plus, les sites Web peuvent placer un fichier témoin pouvant contenir des renseignements personnels dans le navigateur d'un utilisateur. Si le fichier témoin est communiqué à un tiers, les renseignements personnels qu'il contient sont divulgués.

Le terme « fuites sur Internet » désigne ces formes de divulgation en ligne à des tiers par le biais de méthodes telles que les requêtes de recherche Web, les fichiers témoins et autres approches non abordées dans le présent document.

Nos travaux de recherche

En juillet et août 2012, nous avons testé 25 sites populaires auprès de la population canadienne. La plupart des sites étaient assujettis à la LPRPDE, mais nous avons aussi testé un petit nombre de sites exploités par des organisations assujetties à la Loi sur la protection des renseignements personnels.

Nous avons créé quelques comptes de test à partir desquels nous avons soumis des données personnelles comme des coordonnées fictives. Nous avons ensuite vérifié si certaines de ces données, ou toutes, avaient été communiquées à des tiers.

[1] http://w2spconf.com/2011/papers/privacyVsProtection.pdf [en anglais seulement].

Nous avons relevé des préoccupations importantes en matière de protection de la vie privée pour six sites Web et des soucis moindres pour cinq autres. Ces sites semblaient divulguer des renseignements personnels soumis par les utilisateurs lors de l'inscription pour l'ouverture d'un compte. Les 14 autres sites que nous avons testés ne semblaient pas transmettre de renseignements personnels.

Selon notre analyse, les organisations tierces qui ont obtenu nos renseignements personnels appartenaient à trois grandes catégories :

- Les entreprises de publicité (qui sont responsables de fournir des annonces publicitaires de tiers aux sites Web);
- Les sociétés d'analyses Web (qui mesurent, recueillent, analysent et communiquent des données sur l'utilisation des sites Web à des fins comme le marketing et l'amélioration d'aspects d'un site Web);
- Les services de circulaire électronique (qui fournissent des services comme l'envoi de circulaires hebdomadaires à des sites Web. Ces circulaires mettent en vedette des promotions spéciales, qui sont souvent adaptées à une région donnée).

Que s'est il passé ensuite?

La commissaire à la protection de la vie privée a communiqué par écrit avec 11 organisations pour lesquelles nous avions constaté que les sites Web divulguaient des renseignements personnels. Elle leur a demandé d'apporter des précisions sur leurs pratiques et, le cas échéant, d'expliquer la façon dont elles entendaient les modifier pour se conformer aux lois relatives à la protection de la vie privée.

La commissaire a été rassurée par la grande attention que presque toutes les organisations concernées ont accordée à cette question. Elle a constaté des changements positifs à la suite de cette étude qui marque, selon elle, un pas important en vue de s'assurer que les sites Web canadiens obtiennent un consentement explicite pour la collecte, l'utilisation et la communication de renseignements personnels des utilisateurs.

L'équipe de sensibilisation des intervenants a aussi suivi le déroulement de cette étude. Le Commissariat a rencontré des associations et des intervenants de l'industrie travaillant en vue de l'atteinte d'un objectif commun d'amélioration de la conformité en matière de protection de la vie privée.

Cet exercice concret a mis en évidence la nécessité, pour les organisations, de mieux adapter leurs politiques de confidentialité et leurs processus de consentement en fonction de la réalité du monde en ligne d'aujourd'hui. De concert avec ses homologues provinciaux, le Commissariat établira des lignes directrices sur l'obtention d'un consentement explicite en ligne.

3.5.3 *Comprendre l'analyse prédictive*

Les éléments de données que les personnes laissent derrière elles sans le savoir par leur navigation Internet, les échanges sur les médias sociaux, l'utilisation de cartes de fidélité de magasins de détail et beaucoup d'autres activités courantes valent leur pesant d'or pour les entreprises à la recherche de moyens pour cibler leurs efforts de marketing.

En effet, une toute nouvelle tendance appelée l'analyse prédictive consiste à analyser les pistes de données laissées par les personnes afin d'extraire des indices sur leurs habitudes personnelles, leurs préférences et leurs intentions d'achats.

De façon plus générale, l'analyse prédictive est une branche du forage des données qui vise à prédire des probabilités. Il s'agit d'un processus d'analyse Web général qui peut être appliqué dans des domaines aussi divers que la vente au détail pour promouvoir les ventes, le maintien de l'ordre pour prédire les crimes et les programmes de santé pour surveiller les éclosions de maladie.

La nouvelle qu'un géant américain du commerce de détail avait utilisé l'analyse prédictive pour identifier les femmes susceptibles d'être en début de grossesse, et donc, de ce fait, d'être plus attentives aux publicités concernant les articles pour bébé, a permis de mieux saisir le phénomène.

Les outils d'analyse Web, comme la fonction algorithmique de prédiction de la grossesse utilisée par le commerçant américain, étant déployés en arrière-plan, il est difficile, voire impossible, pour les personnes de connaître l'utilisation qui est faite de leurs renseignements personnels.

Qui plus est, ces pratiques deviennent de plus en plus courantes et potentiellement envahissantes.

C'est pour ces raisons que le Commissariat a décidé d'examiner la pratique dans le cadre de son programme de recherche interne, et de produire un rapport qui sera publié au cours de la prochaine année. Ce rapport s'inscrit dans un effort continu pour comprendre la valeur des données massives pour les organisations et réfléchir aux répercussions de ces nouvelles technologies sur la vie privée.

3.5.4 *Tests génétiques offerts en ligne directement aux consommateurs*

Les percées dans les domaines des sciences médicales et des technologies de l'information ont rendu les tests génétiques plus accessibles et abordables. Les gens peuvent désormais se procurer des trousses auprès d'entreprises qui proposent en ligne des services de tests génétiques pour savoir s'ils courent un risque plus élevé de développer certaines maladies courantes, et ce, sans jamais devoir consulter un médecin.

Ces tests génétiques offerts directement aux consommateurs sont de plus en plus populaires, et les compagnies d'assurances y voient une occasion à saisir. Si les tests génétiques peuvent permettre

d'anticiper l'avenir d'une personne, les assureurs sont naturellement désireux de tirer parti de cette information dans leurs évaluations des risques.

Il n'existe aucune loi au Canada qui traite explicitement de l'utilisation des résultats des tests génétiques à des fins non médicales, telles que l'évaluation des risques au motif d'assurances. Toutefois, en vertu de la LPRPDE, toute collecte de renseignements personnels à des fins commerciales doit respecter le principe de la « limitation de la collecte ». La *Loi* précise en outre qu'une organisation ne peut « recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ».

Pour nous aider à comprendre et à évaluer ce domaine en évolution rapide, que nous avons défini, il y a quelques années, comme l'un de nos quatre domaines prioritaires, le Commissariat a commandé deux documents à des experts du milieu universitaire. Les documents, qui sont disponibles sur notre site Web, ont été préparés par M. Angus Macdonald, professeur au département des mathématiques actuarielles et des statistiques et à l'Institut Maxwell des sciences mathématiques de l'Université Heriot Watt, à Édimbourg, ainsi que M. Michael Hoy, professeur au département des sciences économiques et de la finance à l'Université de Guelph, Ontario, et M[me] Maureen Durnin, chercheuse indépendante à la même université.

Nous avons également demandé au D[r] Steve Scherer, directeur du Centre de génomique appliquée de l'Hôpital pour enfants de Toronto, de répondre à une série de questions sur la valeur prédictive des renseignements génétiques. Les questions et réponses de cet entretien sont également affichées sur notre site Web.

Pour préciser davantage nos idées sur la question, nous avons invité des experts à participer à une table ronde pour discuter des documents de recherche commandés et de la position de l'Association canadienne des compagnies d'assurances de personnes sur l'utilisation des résultats de tests génétiques.

3.6 ÉTABLIR UN DIALOGUE AVEC LES ENTREPRISES

Un volet essentiel de notre mandat consiste à établir un dialogue avec les intervenants — pour écouter leurs préoccupations et leur communiquer notre savoir en ce qui a trait à la protection de la vie privée. En 2012, des employés du Commissariat ont présenté 101 discours lors d'événements comme le Forum Droit du commerce et Internet, la Conférence sur les communications des entreprises canadiennes, le lancement national du Centre de soutien aux victimes de vol d'identité du Canada, le Symposium sur le droit à la vie privée et à l'accès à l'information organisé par l'Association du Barreau canadien et la Conférence des professionnels canadiens de la communication de l'Association internationale des professionnels de la communication.

3.6.1 *Le bureau de Toronto*

Notre bureau de Toronto s'impose de plus en plus dans la région du Grand Toronto en ce qui a trait a des activités de base du Commissariat à la protection de la vie privée du Canada.

Nous avons choisi d'établir une succursale de notre bureau d'Ottawa à Toronto parce qu'on y retrouve les sièges sociaux de nombre d'associations industrielles et d'organisations de même que de nombreux intervenants concernés par la LPRPDE. Depuis lors, la partie du bureau de Toronto s'est élargie pour comprendre la collaboration avec un éventail d'intervenants en vue d'améliorer le respect par l'industrie de la LPRPDE, pour le bénéfice des Canadiennes et Canadiens.

Le fait d'être à l'écoute des intervenants permet au Commissariat de mieux comprendre les questions et les priorités des entreprises. Cet engagement tangible nous fournit aussi le contexte nécessaire pour nous assurer que les documents d'orientation et de communication que nous produisons sont opportuns et pertinents.

Un objectif clé de notre effort de sensibilisation est d'encourager davantage le respect volontaire de loi sur la protection des renseignements personnels applicable au secteur privé, donnant ainsi lieu à moins d'enquêtes sur des plaintes. Le dialogue continu et l'échange d'information permettront aussi d'accroître la sensibilisation et la protection de la vie privée des Canadiennes et Canadiens.

Dans le cadre de nos activités de sensibilisation, les entreprises nous ont dit souhaiter plus que tout obtenir une liste facile à consulter des pièges concernant la protection de la vie privée et la façon de les éviter. En nous fondant sur l'examen des plaintes que nous avons reçues en vertu de la LPRPDE ces dernières années, nous avons donc dressé cette liste de dix conseils pour aider les organisations à éviter les problèmes les plus communément signalés en matière de protection de la vie privée :

1) Affichez sur votre site Web les coordonnées du responsable de la protection de la vie privée de votre organisation;
2) Donnez une formation sur la protection de la vie privée à vos employés;
3) Assumez la responsabilité des faits et gestes de vos employés;
4) Limitez la collecte de renseignements personnels;
5) Rendez optionnelle l'utilisation du numéro d'assurance sociale en tant qu'identifiant;
6) Permis de conduire : vous pouvez l'examiner, mais ne prenez pas note du numéro qui y est inscrit;
7) Dites à vos clients que vous avez installé des caméras de sécurité, le cas échéant;
8) Protégez les renseignements personnels;
9) Répondez aux demandes d'accès aux renseignements personnels;
10) Informez adéquatement les utilisateurs au sujet de la collecte et de l'utilisation des renseignements personnels

3.6.2 *Sondage auprès des entreprises*

Au début de 2012, nous avons rendu public un autre grand sondage sur les entreprises, qui a révélé que les entreprises canadiennes stockent de plus en plus de renseignements personnels sur des dispositifs numériques, mais que nombre d'entre elles n'appliquent pas les outils ou les pratiques nécessaires pour bien les protéger.

Le sondage d'opinion publique de 2012 sur les entreprises canadiennes et les renseignements personnels (http://www.priv.gc.ca/information/por-rop/2012/por_2012_01_f.pdf)

Le sondage d'opinion publique de 2012 sur les entreprises canadiennes et les renseignements personnels faisait suite aux sondages que nous avons réalisés en 2007 et 2010. Les sondages nous aident à comprendre comment les organisations du secteur privé envisagent les défis en matière de protection de la vie privée et y répondent.

Un sondage téléphonique mené auprès de 1 006 entreprises de partout au Canada — de tailles différentes et appartenant à divers secteurs — a révélé que les organisations stockent des renseignements personnels dans différents dispositifs numériques, comme des ordinateurs de bureau (55 %), des serveurs (47 %) et des appareils portatifs (23 %).

Près des trois quarts d'entre elles (73 %) utilisent des outils technologiques comme des mots de passe, un logiciel de cryptage ou des pare-feux pour prévenir un accès non autorisé aux renseignements personnels stockés dans ces dispositifs.

Cependant, le sondage indique également que plusieurs entreprises pourraient ne pas utiliser les mécanismes de protection associés à ces technologies de façon optimale.

Par exemple, les mots de passe représentent l'outil technologique le plus souvent employé par les entreprises pour protéger les renseignements personnels (96 % de toutes les mesures utilisées). Toutefois, parmi les entreprises qui utilisent des mots de passe, près de quatre sur dix ne disposent pas des mesures de contrôle nécessaires pour veiller à ce que ces mots de passe soient difficiles à deviner, et 27 % d'entre elles n'exigent jamais que leurs employés changent leurs mots de passe.

Le sondage a également révélé que près du quart des entreprises stockent des renseignements personnels sur des dispositifs portables, comme des ordinateurs portatifs, des clés USB ou des tablettes électroniques, qui sont plus vulnérables au vol et plus souvent perdus que les ordinateurs de bureau. Près de la moitié des entreprises qui stockent des données sur de tels dispositifs (48 %) ont indiqué ne pas avoir recours au cryptage pour les protéger.

En ce qui concerne les attitudes à l'égard de la protection des renseignements personnels, le sondage a donné des résultats mitigés.

Par exemple, tandis que les trois quarts des entreprises (77 %) ont dit accorder beaucoup d'importance à la protection des renseignements personnels, seules six entreprises sur dix (62 %) ont mis en place une politique concernant la protection de la vie privée, la moitié (48 %) disposent de procédures relatives au traitement des plaintes déposées par des clients qui estiment que leurs renseignements personnels ont été gérés de façon inappropriée, et le tiers des entreprises (32 %) ont donné à leurs employés une formation sur les pratiques et les lois en matière de protection de la vie privée.

En revanche, la majorité des entreprises (57 %) qui disposent d'une politique sur la protection des renseignements personnels en font la mise à jour au moins une fois par année, et près de quatre entreprises sur dix (39 %) considèrent la protection de la vie privée comme un avantage concurrentiel.

3.7 LIGNES DIRECTRICES, POLITIQUES ET OUTILS

Le Commissariat réalise ou commande des travaux de recherche, discute et traite avec les provinces, collabore avec des partenaires internationaux et dialogue avec le secteur privé, à la fois par l'intermédiaire de son bureau principal d'Ottawa et de celui de Toronto. Toutes ces activités alimentent l'élaboration de nos lignes directrices, bulletins d'interprétation, énoncés de politique, fiches d'information et autres outils.

Le Commissariat croit que le fait de prêter une oreille attentive aux intervenants lui permet d'assurer la pertinence, l'opportunité et l'utilité de ses produits d'orientation. Ce qui, en retour, augmente la probabilité du respect des lois et diminue l'incidence de plaintes — un net avantage pour les entreprises, la population canadienne et le Commissariat.

Cette section décrit les principaux conseils et autres outils que nous avons diffusés en 2012. Ils s'ajoutent à ces trois publications, décrites ailleurs dans ce rapport :

- *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, produit en association avec nos homologues de l'Alberta et de la Colombie-Britannique. Le document, qui est accompagné d'un bulletin d'interprétation connexe, fait état de nos attentes à l'égard des programmes de protection de la vie privée et de la nécessité, pour les organisations, de prendre des engagements et de mettre en place des mesures de contrôle quant aux programmes. Pour de plus amples renseignements, veuillez consulter la section 2.1 du présent rapport.
- *Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée* a été publié par le Commissariat en octobre 2012. Il vise à convaincre les concepteurs d'applications mobiles que les mesures de protection de la vie privée profitent aux utilisateurs et les amènent à faire confiance au produit. Les lignes directrices sont décrites plus en détail dans un encadré de la section 2.7 de ce rapport.
- Nos dix principaux conseils pour éviter les pièges les plus répandus en matière de protection de la vie privée sont décrits dans la section 3.6.1 ci-dessus.

3.7.1 *Politique relative à la publicité comportementale en ligne*

La publicité comportementale en ligne est une pratique qui consiste à suivre les activités sur le Web de personnes, dans plusieurs sites et au fil du temps, pour connaître leurs intérêts et leur présenter des publicités ciblées. Parmi les secteurs intéressés par le suivi, le profilage et le ciblage en ligne (désignés collectivement comme la publicité comportementale en ligne), il y a l'industrie de la publicité, les concepteurs de navigateurs et les exploitants de sites Web.

La pratique utilise des moyens technologiques comme les fichiers témoins, les pixels espions, les supertémoins, les fichiers témoins « zombie » et les données des appareils pour recueillir et utiliser des renseignements sur les activités d'une personne sur le Web. Le Commissariat considère qu'il y a, parmi les données recueillies, des renseignements personnels qui relèvent de l'application de la LPRPDE.

À cette fin, nous avons publié en décembre 2011 des *Lignes directrices sur la publicité comportementale en ligne* pour régir la collecte et l'utilisation appropriées des données dans le cadre de cette pratique. Ensuite, pour expliquer plus en détail le fondement de nos lignes directrices, nous les avons fait suivre en 2012 d'une politique.

Lignes directrices sur la publicité comportementale en ligne (http://www.priv.gc.ca/information/guide/2012/bg_ba_1206_f.asp)

Entre autres choses, la politique exhorte les entreprises qui ont recours à la publicité comportementale en ligne à ne pas suivre les activités en ligne des enfants. Pour ce qui est des adultes dont les activités peuvent être suivies, les organisations ne devraient pas utiliser de moyens technologiques comme les fichiers témoins « zombie », auxquels il est difficile, voire impossible, de refuser de consentir.

Voici les conditions nécessaires à la mise en place d'une option valide de refus de consentir :

- Les utilisateurs doivent être informés des objectifs de la publicité comportementale en ligne de façon claire et compréhensible — ces objectifs ne doivent pas être dissimulés à l'intérieur d'une politique de confidentialité. Les organisations devraient envisager de communiquer avec les utilisateurs de la façon la plus transparente possible, notamment à l'aide de bannières en ligne, d'approches par étapes et d'outils interactifs.

- Les utilisateurs devraient être informés de ces fins au moment de la collecte ou avant, et recevoir de l'information sur les diverses parties qui participent au processus de publicité comportementale en ligne.

- Les utilisateurs doivent pouvoir facilement se soustraire à la pratique, idéalement au moment de la collecte des renseignements ou avant. Le refus de consentir doit être immédiat et durable.

- Les renseignements personnels recueillis et utilisés devraient être limités, dans la mesure du possible, à des informations non sensibles. Les renseignements médicaux et autres informations délicates devraient être exclus.

- Les renseignements recueillis et utilisés devraient être détruits dès que possible ou convertis de manière à ce qu'il soit impossible de les mettre en correspondance avec l'utilisateur qui les a fournis.

3.7.2 *Document d'orientation sur l'infonuagique à l'intention des PME*

Beaucoup de petites et moyennes entreprises (PME) ont adopté massivement des solutions d'infonuagique qui leur permettent de louer une partie de la grande capacité de traitement informatique et de stockage d'une organisation beaucoup plus importante. En adoptant des solutions d'infonuagique, les entreprises délèguent effectivement leurs problèmes de maintenance et de mise à niveau des TI à quelqu'un d'autre.

Cependant, les PME doivent savoir que tous les avantages que semble offrir l'externalisation de leur informatique à un colosse multinational spécialisé dans ces activités s'accompagnent également de risques. Un de ces risques est que les PME pourraient perdre la maîtrise des renseignements personnels recueillis dont elles sont responsables, en dernier ressort, en vertu de la LPRPDE.

Pour aider les PME à comprendre leurs responsabilités en matière de protection de la vie privée et évaluer les risques et les conséquences de l'externalisation de la gestion des renseignements personnels à un service d'infonuagique, le Commissariat a collaboré avec ses homologues de l'Alberta et de la Colombie-Britannique à la préparation d'un nouveau document d'orientation.

Le document d'orientation intitulé *L'infonuagique pour les petites et moyennes entreprises : Responsabilités et points importants touchant la protection des renseignements personnels* rappelle aux entreprises, quelle que soit leur taille, qu'elles sont responsables, en dernier ressort, des renseignements personnels qu'elles recueillent, utilisent et communiquent, même lorsque la gestion des renseignements personnels a été confiée à un fournisseur de services d'infonuagique externe.

L'infonuagique pour les petites et moyennes entreprises : Responsabilités et points importants touchant la protection des renseignements personnels (http://www.priv.gc.ca/information/pub/gd_cc_201206_f.asp)

Le document contient une série de questions que les PME devraient se poser lorsqu'elles envisagent d'avoir recours à des services d'infonuagique. Il recommande aux PME d'effectuer des évaluations minutieuses et d'utiliser des moyens contractuels ou d'autres moyens pour assurer que le traitement et la protection des renseignements personnels

par le fournisseur de services d'infonuagique sont appropriés.

Le document met particulièrement en garde les PME contre les contrats du type « à prendre ou à laisser », qui peuvent prévoir des pratiques d'utilisation et de conservation plus souples, ou renfermer des dispositions standard trop laxistes pour permettre aux PME de s'acquitter de leurs obligations à l'égard de la protection de la vie privée.

Le document incite également les PME à réfléchir aux mesures de sécurité, telles que le cryptage et les mesures de contrôle d'accès, et à tenir compte de l'application de la loi par différentes administrations.

La transparence étant un élément clé, on encourage les PME à comprendre leurs responsabilités, et à s'assurer de répondre aux attentes des clients.

3.7.3 *Trousse d'urgence pour la protection des renseignements personnels*

Des lois régissant la collecte, l'utilisation et la communication de renseignements personnels existent à tous les échelons du gouvernement, tant pour les secteurs public que privé. Elles permettent toutes la communication appropriée de renseignements personnels en cas d'urgence — un fait qui est souvent mal compris en situation de stress et d'urgence.

En situation d'urgence, il est possible que l'on demande à certaines organisations qui sont assujetties à la LPRPDE de donner aux autorités des renseignements personnels sur des clients, sans le consentement des personnes concernées. Par exemple, on pourrait demander à une compagnie aérienne ou à un cabinet de dentiste des renseignements personnels pour aider les intervenants en cas d'urgence à déterminer si des personnes manquent à l'appel ou identifier des victimes.

Au cours de la dernière année, nous avons consulté nos homologues provinciaux et territoriaux en vue de l'élaboration d'une trousse d'urgence pour la protection des renseignements personnels afin d'aider les organisations à traiter correctement les renseignements personnels avant, pendant et après une urgence.

La trousse, qui a été rendue publique en mai 2013, explique que les lois sur la protection de la vie privée ne devraient pas faire obstacle à l'action et à la communication appropriée de renseignements en cas d'urgence. Elle comprend des listes de contrôle et des questions fréquemment posées au sujet de divers éléments d'information importants, tels que les autorités avec lesquelles la communication de renseignements personnels est autorisée en vertu de la loi.

Le document d'orientation a été élaboré dans la foulée de la *Résolution sur la protection des données et les catastrophes naturelles majeures* qui a été adoptée lors de la 33e Conférence internationale des commissaires à la protection des données et de la vie privée en novembre 2011.

La LPRPDE et l'évolution du droit à la vie privée

La LPRPDE a été adoptée en 2000 et est entrée en vigueur au cours des trois années subséquentes. La loi compte de nombreux points forts, notamment des principes neutres sur le plan technologique, qui lui ont permis de s'adapter aux nouveaux défis.

Ces dernières années, toutefois, il est devenu évident que des améliorations fondamentales doivent être apportées à la LPRPDE pour qu'elle puisse suivre le rythme des changements profonds qui s'opèrent dans le domaine de la protection de la vie privée.

Une des menaces les plus graves pour les renseignements personnels tient à la grande quantité de données détenues par bon nombre de géants mondiaux de l'économie numérique. Il devient de plus en plus difficile de protéger l'information contre les atteintes accidentelles à la sécurité des données et les cybercriminels professionnels.

Par ailleurs, les organisations reconnaissent de plus en plus la valeur des renseignements personnels qu'elles détiennent et renforcent leur compétitivité au moyen de nouvelles utilisations des données, qui sont parfois inattendues, voire impopulaires.

Si les choses tournent mal, elles peuvent dégénérer à grande échelle. Lorsque nous enquêtons, nous découvrons souvent que les organisations n'ont pas anticipé les problèmes relatifs à la protection de la vie privée qu'elles ont provoqués en précipitant l'arrivée sur le marché de nouveaux produits ou services utilisant un grand volume de données.

Pire encore, lorsque nous intervenons en recommandant des améliorations, nous avons trop souvent affaire à une réponse léthargique contre laquelle nous ne pouvons pas grand chose. Bien que les entreprises puissent finir par accepter les recommandations qui visent à améliorer leurs pratiques en matière de protection de la vie privée, le processus pour y parvenir est souvent laborieux et chronophage. De plus, le travail nécessaire pour assurer que les recommandations sont, en fin de compte, mises en œuvre entraîne des coûts

supplémentaires, car le Commissariat ne dispose pas des moyens légaux voulus pour obtenir les résultats souhaités en matière de protection de la vie privée, et encore moins pour accélérer les choses.

Nous avons, au cours des dernières années, tâché de tirer le meilleur parti possible des pouvoirs dont dispose la commissaire en vertu de la loi pour relever les nouveaux défis auxquels nous avons été confrontés. Nous estimons avoir accompli, au moyen de ces outils, un travail relativement efficace, y compris pour ce qui est de déposer plus de plaintes, de réaliser des vérifications de la conformité et d'exercer notre pouvoir discrétionnaire pour nommer des personnes lorsqu'il en va de l'intérêt du public.

Et pourtant, il est devenu évident que même cela ne suffit pas. La loi manque de mesures incitatives adéquates pour pousser les organisations à investir massivement dans la protection de la vie privée. En effet, les organisations peuvent toujours accepter de modifier leurs pratiques après avoir fait l'objet d'une enquête ou d'une vérification, sans pour autant mettre en œuvre les recommandations — ou ne le faire qu'après avoir été talonnées pendant un long moment. La loi ne prévoyant aucune possibilité d'imposer des amendes ou d'ordonner des dommages intérêts, les organisations encourent peu de sanctions monétaires en cas de non-conformité à la LPRPDE — sauf peut être les honoraires d'un avocat ou d'autres conseillers.

Par conséquent, nous sommes convaincus qu'étant donné le rayonnement mondial des plus puissantes entreprises d'aujourd'hui, le Canada doit se doter de pouvoirs comparables à ceux d'autres pays pour renforcer la protection de la vie privée.

En effet, au cours des dernières décennies, les autorités de protection des données d'autres pays se sont vu conférer des pouvoirs d'application accrus, notamment le pouvoir d'imposer des sanctions pécuniaires importantes.

Le Canada ne peut pas se permettre de prendre du retard en acceptant que ceux qui ne respectent pas les lois canadiennes en matière de protection de la vie privée ne subissent que des conséquences négligeables. De bonnes pratiques en matière de protection de la vie privée sont essentielles à la confiance des consommateurs, sur laquelle repose une économie numérique florissante.

C'est pourquoi le Commissariat a préconisé l'octroi de pouvoirs accrus en vertu de la LPRPDE, notamment le signalement obligatoire des atteintes, les conséquences financières en cas de non conformité et d'autres changements au modèle d'application.

Des mécanismes d'application renforcés inciteraient les entreprises à gérer promptement les risques liés à la protection de la vie privée et à prendre leur responsabilité à l'égard des incidents dans ce domaine. Ces mécanismes, jumelés à une responsabilisation accrue, encourageraient les organisations à adopter dès le départ des mesures visant à atténuer les risques et à assurer la conformité à la loi.

Tout cela permettrait aux entreprises de faire preuve d'esprit d'innovation et de concurrence, tout en

maintenant la confiance des consommateurs à l'égard des entreprises et de leurs produits.

Ce chapitre traite de nos efforts constants pour que la LPRPDE reste à la hauteur des défis d'aujourd'hui et que la commissaire à la protection de la vie privée soit dotée des pouvoirs nécessaires pour la faire appliquer.

Il fait également état d'autres échanges que nous avons eus avec le Parlement, institution dont relève la commissaire à la protection de la vie privée et le Commissariat, y compris une série d'audiences sur l'incidence des médias sociaux sur la protection de la vie privée.

Plus loin dans le chapitre, nous mettons en relief notre travail devant les tribunaux, qui a porté principalement sur le renforcement et le soutien du respect, par les organisations, de leurs droits et obligations en matière de protection de la vie privée en vertu de la LPRPDE. Cette section aborde aussi la comparution du Commissariat devant la Cour suprême du Canada, où nous avons préconisé la mise en place d'un cadre visant à assurer un équilibre entre le droit à la vie privée et le principe de la transparence judiciaire dans les affaires concernant les adolescents et les médias sociaux.

Nos efforts en 2012 se sont également étendus au-delà de la Cour fédérale et des systèmes législatifs pour englober le travail avec les provinces et les territoires, ainsi qu'avec d'autres autorités internationales chargées de la protection des données et organisations connexes. Ces efforts sont aussi présentés en détail dans le présent chapitre.

4.1 AU PARLEMENT

L'année 2012 a été chargée pour notre équipe des affaires parlementaires. Nous avons comparu dix fois devant des comités des deux chambres du Parlement et avons soumis trois mémoires sur des affaires qui touchaient à la protection de la vie privée.

Nous avons également analysé 14 projets de loi pour évaluer leurs éventuelles répercussions sur la protection de la vie privée, notamment le projet de loi C-30, la *Loi sur la protection des enfants contre les cyberprédateurs*. Nous avons cerné des répercussions claires pour la LPRPDE dans ce projet de loi, car de nombreuses dispositions auraient interagi avec la disposition de l'autorité légitime de la *Loi*.

La commissaire à la protection de la vie privée est une agente du Parlement. Elle relève directement du Parlement plutôt que du gouvernement en place. Le groupe des affaires parlementaires du Commissariat examine et analyse les initiatives législatives et appuie la commissaire pour ce qui est des comparutions devant le Parlement et de ses relations avec les parlementaires.

Cependant, au début de 2013, le gouvernement a annoncé qu'il n'irait pas de l'avant avec cette loi.

En outre, nous avons répondu à 57 demandes officielles de la part des députés et des sénateurs. Neuf de ces demandes concernaient la LPRPDE.

À trois reprises nous avons été invités à comparaître devant le Comité permanent de l'accès à l'information, de la protection des renseignements et de l'éthique (ETHI). On nous a aussi demandé d'offrir à une séance d'information sur le projet de loi C-12, *la Loi protégeant les renseignements personnels des Canadiens*. Le projet de loi C-12 vise à modifier la LPRPDE pour y ajouter les exigences relatives au signalement des atteintes et à élargir les motifs pour lesquels les organismes d'application de la loi peuvent demander aux organisations de leur communiquer des renseignements personnels.

En outre, le Commissariat a dû répondre à des questions émanant des parlementaires concernant la LPRPDE, l'utilisation des renseignements personnels par les entreprises de production de déclarations de revenus ou de rapports de solvabilité, les entreprises américaines utilisant les numéros d'assurance sociale canadiens pour offrir des services au Canada et les renseignements personnels utilisés sur les sites Web qui pourraient avoir des conséquences négatives sur la réputation des personnes.

4.1.1 *La commissaire témoigne lors des audiences sur la vie privée et les médias sociaux*

En mai 2012, le Comité permanent de l'accès à l'information, de la protection des renseignements et de l'éthique (ETHI) a lancé un examen pour déterminer dans quelle mesure les entreprises de médias sociaux protègent la vie privée et les renseignements personnels des Canadiennes et Canadiens.

Ces audiences ont réuni des universitaires, des défenseurs des droits et des représentants de l'industrie, notamment les géants d'Internet que sont Google, Facebook et Twitter. La commissaire Stoddart, accompagnée de la commissaire adjointe, Chantal Bernier, et de membres de son personnel, a été invitée à faire une présentation au début de l'étude ainsi qu'à dresser un bilan.

La commissaire a présenté un cadre pouvant permettre au Comité de concentrer son étude, suggérant que les enjeux clés pour la protection de la vie privée dans le contexte des médias sociaux résident dans les limites de la collecte et de la conservation des renseignements personnels, la garantie que les personnes fournissent un consentement valable pour la collecte de leurs renseignements personnels, et les responsabilités en matière de protection de la vie privée.

Elle a invité les gouvernements, les éducateurs et les collectivités à se concentrer sur l'éducation numérique des Canadiennes et Canadiens de tous âges, pour inclure notamment les enjeux sociétaux et éthiques plus vastes amenés par les nouvelles technologies de l'information. Sans dispenser les entreprises exerçant des activités sur Internet de leurs obligations en vertu des lois sur la protection de la vie privée, la culture numérique permet aux personnes de comprendre que les renseignements sur elles-mêmes ou sur autrui qu'elles publient en ligne peuvent y rester à jamais.

La commissaire a par ailleurs déclaré que la LPRPDE pourrait devoir être renforcée afin d'encourager les entreprises à s'y conformer davantage et à faire preuve

d'une plus grande responsabilité. Elle a fait remarquer que les pouvoirs en matière d'application de la loi de plusieurs autorités de la protection des données à l'échelle internationale avaient été renforcés. La loi préconise actuellement une approche « douce » fondée sur des recommandations non contraignantes, où le risque le plus élevé pour la réputation d'une organisation prend la forme d'une attention négative que l'organisation peut attirer lorsque la commissaire exerce son pouvoir de la nommer dans l'intérêt public.

Si la plupart des témoins ont convenu des problèmes relatifs à la protection de la vie privée posés par les médias sociaux, les points de vue différaient quant à la pertinence des outils disponibles pour y remédier. À l'exception de certains représentants de l'industrie et des entreprises, la plupart des universitaires, des défenseurs des droits, une association de l'industrie et les commissaires provinciaux de la Colombie-Britannique et de l'Ontario estiment que la commissaire fédérale doit disposer de pouvoirs renforcés.

Des témoins ont également fait état de leur désaccord quant à la pertinence d'une initiative législative visant à rendre obligatoire le signalement des atteintes à la protection des données. Certains représentants du secteur des affaires ont en effet expliqué que de telles mesures imposeraient un fardeau excessif aux petites organisations. La commissaire n'était toutefois pas d'accord. Elle a indiqué que, compte tenu des vastes quantités de renseignements personnels détenues par les organisations sur des plateformes de plus en plus complexes, le risque d'atteintes importantes et d'utilisations potentiellement envahissantes de ces renseignements personnels exige la mise en place de mesures de sécurité et de conséquences adaptées qui ne sont pas actuellement prévues par la LPRPDE.

Le rapport final du Comité devrait être déposé à la Chambre des communes en avril 2013.

4.2 DEVANT LES TRIBUNAUX

L'an dernier, le Commissariat a participé à plusieurs poursuites devant la Cour fédérale et a comparu devant la Cour suprême du Canada. Cette section décrit une demande que nous avons déposée, ainsi que les demandes déposées par des tiers à notre encontre et les occasions où nous avons agi à titre d'intervenant devant le tribunal.

La section 1.3 du présent rapport décrit une poursuite additionnelle impliquant Nexopia, le site de réseautage social destiné aux jeunes.

4.2.1 *Commissaire à la protection de la vie privée du Canada c. Association of American Medical Colleges* (numéro de dossier de la Cour fédérale : T-1712-10)

En 2012, le Commissariat a trouvé une issue favorable à une demande que nous avions présentée à la Cour fédérale contre l'Association of American Medical Colleges (AAMC) en 2010. Notre demande faisait suite à une enquête que nous avions menée concernant la pratique de l'AAMC visant à recueillir les empreintes digitales et d'autres renseignements

personnels des candidats au Medical College Admission Test (MCAT).

L'AAMC possède et administre le MCAT. L'AAMC faisait appel à un tiers pour recueillir les empreintes digitales et d'autres renseignements personnels des candidats au MCAT. Même si les empreintes digitales étaient converties en un gabarit numérique, l'AAMC conservait l'image des empreintes pour maintenir l'intégrité de sa base de données d'empreintes digitales.

Une personne s'est plainte au Commissariat de la collecte par l'AAMC de renseignements personnels dans le cadre du MCAT. Elle estimait que la collecte d'empreintes digitales n'était pas nécessaire et a exprimé ses préoccupations quant à la conservation et à la protection des données relatives aux empreintes digitales.

À la suite des éléments découverts durant notre enquête, nous avons conclu que des moyens portant moins atteinte à la vie privée permettraient à l'AAMC d'atteindre ses objectifs.

De plus, nous avons déterminé que l'AAMC conservait trop longtemps les renseignements personnels recueillis; et que l'association devait se doter d'un programme garantissant la sécurité des renseignements et continuer de prévoir la protection des renseignements dans ses contrats avec les tiers fournisseurs de services.

L'AAMC a apporté certains changements. Elle a notamment mis en place des mesures pour informer les candidats de la collecte des renseignements personnels et pour limiter la conservation des renseignements personnels recueillis lors des tests à cinq ans.

L'organisation a également accepté nos recommandations sur la protection des renseignements recueillis.

Cependant, l'AAMC a indiqué qu'elle continuerait à recueillir les empreintes digitales des candidats, ainsi que les photographies et une numérisation de leur permis de conduire. L'organisation considère que ces renseignements personnels sont nécessaires pour empêcher des personnes de passer l'examen de manière frauduleuse au nom de quelqu'un d'autre.

La commissaire à la protection de la vie privée s'est donc adressée à la Cour fédérale en vue d'obtenir une ordonnance obligeant l'AAMC à utiliser des moyens portant moins atteinte à la vie privée pour assurer l'intégrité de l'examen.

Pendant l'examen de la demande et les séances de médiation, l'AAMC a présenté d'autres éléments de preuve et arguments démontrant l'étendue du problème posé par les personnes qui se présentent à l'épreuve à la place des candidats inscrits et par d'autres formes d'inconduite pour justifier la prise de mesures visant à réduire le risque de fraude.

Le Commissariat a finalement reconnu, au vu des éléments de preuve présentés, qu'il existait un risque important de fraude dans le contexte de l'administration du MCAT, et que l'AAMC avait fait la preuve de la nécessité de recueillir et d'utiliser une quantité limitée de renseignements personnels pour

protéger l'intégrité du MCAT, empêcher que des personnes passent l'épreuve à la place des candidats inscrits et enquêter en cas de fautes présumées pendant le déroulement de l'examen.

Le Commissariat et l'AAMC ont convenu d'une solution qui a abouti à un règlement des questions soulevées dans la demande.

L'AAMC a accepté de limiter les renseignements personnels recueillis et de cesser d'enregistrer les renseignements personnels contenus sur les pièces d'identité gouvernementales présentées pour confirmer l'identité des candidats.

L'association a également accepté de recueillir et de conserver les renseignements relatifs aux empreintes digitales en format numérique seulement. Toutes les images des empreintes digitales numérisées seront converties en un gabarit numérique unique et conservées de manière sécurisée. De même, les renseignements personnels des candidats seront conservés pendant au maximum cinq ans.

De l'avis de la commissaire, le résultat répond aux préoccupations concernant le respect tant de la vie privée que du besoin de l'AAMC de protéger l'intégrité du MCAT, dont les enjeux sont grands.

4.2.2 *X c. Banque Toronto-Dominion et al* (numéro de dossier de la Cour fédérale : T 2123-11)

Deux personnes se sont plaintes au Commissariat du fait que la Banque Toronto Dominion aurait communiqué une déclaration concernant uniquement le prêt hypothécaire aux avocats représentant une société recouvrant une dette des personnes à deux occasions en 2003 et 2008.

À la suite d'une enquête, la commissaire adjointe à la protection de la vie privée a estimé qu'en 2003, la banque avait divulgué les renseignements personnels des plaignants sans leur consentement et que cet aspect de la plainte était fondé.

La commissaire adjointe à la protection de la vie privée n'a découvert aucune preuve selon laquelle la banque était impliquée dans la seconde divulgation en 2008. La banque a accepté d'offrir une nouvelle formation à ses employés et de leur rappeler l'importance de préserver la confidentialité des renseignements concernant les clients.

Le 30 décembre 2011, les plaignants ont déposé un avis de requête à la Cour fédérale en vertu de l'article 14 de la LPRPDE, afin de solliciter des dommages-intérêts auprès de la banque. La banque a présenté une requête en radiation de la demande faisant valoir que la demande était irrecevable en vertu d'une loi de l'Alberta sur la prescription.

Le 1er mai 2012, la commissaire à la protection de la vie privée s'est vu accorder le droit d'intervenir en qualité de partie à l'instance afin de traiter des questions soulevées par la requête en radiation de la banque. Toutefois, le 12 septembre 2012, les plaignants et la banque ont conclu un accord et la demande a été rejetée.

4.2.3 Demandes de contrôle judiciaire : *X c. commissaire à la protection de la vie privée du Canada*

(numéros de dossier de la Cour fédérale : T-1587-11 et T-1588-11)

Une personne s'était plainte au Commissariat que le fournisseur de services d'orientation de son ancien employeur aurait communiqué des renseignements à son employeur qui, à son tour, les aurait communiqués à d'autres employés, au médecin du plaignant et à un médecin examinateur indépendant.

L'enquête du Commissariat a révélé que les plaintes n'étaient pas fondées et il en a été mention dans le rapport annuel de l'année dernière.

Le 27 septembre 2011, le plaignant a présenté deux demandes de contrôle judiciaire, dans lesquelles il demandait la révision de deux rapports de conclusions rédigés par le Commissariat concernant les plaintes. Le requérant alléguait que la commissaire n'aurait pas observé les principes d'équité procédurale, qu'elle aurait rendu une décision fondée sur une conclusion de fait erronée et qu'elle aurait agi ou omis d'agir en raison d'une fraude ou de faux témoignages.

Le 15 janvier 2013, la Cour fédérale a rejeté les demandes. La Cour a déterminé qu'il n'y avait pas de preuve d'une atteinte à l'équité procédurale et que l'article 14 de la LPRPDE offrait au requérant une autre voie de recours appropriée eu égard aux circonstances. Elle a donc refusé d'effectuer un contrôle judiciaire des rapports de conclusions de la commissaire.

4.2.4 Demande de contrôle judiciaire : *X c. procureur général du Canada et commissaire à la protection de la vie privée du Canada*

(numéro de dossier de la Cour fédérale : T-1588-12)

Il s'agit d'une demande de contrôle judiciaire relative à l'enquête du Commissariat sur une plainte alléguant qu'une organisation aurait indûment refusé au plaignant l'accès à ses renseignements personnels.

Après enquête, le Commissariat a conclu que la plainte était fondée et résolue.

Toutefois, le 27 août 2012, le plaignant a présenté une demande de contrôle judiciaire, espérant que son dossier de plainte soit rouvert.

Au moment de la rédaction du présent rapport, la personne n'a pas produit de preuve par affidavit à l'appui de sa demande ou pris d'autres mesures.

4.2.5 Intervention devant la Cour suprême du Canada : *X c. Bragg Communications Inc.* (numéro de dossier de la Cour suprême du Canada : 34 240)

En 2012, le Commissariat a demandé et reçu l'autorisation d'intervenir dans une affaire devant la Cour suprême du Canada qui soulevait diverses questions importantes liées à la protection de la vie privée.

L'affaire, intentée au nom d'une jeune fille de 15 ans par le père de celle-ci, concernait un faux profil Facebook créé sur la jeune fille par une personne

inconnue. Le faux profil Facebook contenait de l'information sur l'apparence physique de la requérante et ses présumées activités et préférences sexuelles.

La requérante a obtenu l'adresse IP du compte utilisé pour publier le faux profil et a demandé une ordonnance de la Cour exigeant que le fournisseur d'accès Internet local divulgue l'identité du titulaire du compte associé à l'adresse IP en question.

Elle a également demandé une ordonnance de confidentialité qui lui permettrait d'utiliser un pseudonyme et une interdiction partielle de publication afin d'empêcher le public de connaître le contenu du faux profil Facebook.

Le tribunal de première instance a accordé l'ordonnance visant à divulguer l'identité du titulaire de l'adresse IP en question, mais a rejeté les demandes d'ordonnance de confidentialité et d'interdiction partielle de publication introduites par la requérante.

Dès lors, afin d'obtenir les renseignements, la requérante devait renoncer à son anonymat.

La Cour suprême de Nouvelle-Écosse et la Cour d'appel ont rejeté les demandes d'ordonnance de confidentialité et d'interdiction partielle de publication introduites par la requérante, en grande partie parce qu'elles ont estimé que la requérante n'avait pas apporté suffisamment de preuves concernant le préjudice qu'elle subirait si la réparation souhaitée ne lui était pas accordée.

La requérante a finalement présenté un appel auprès de la Cour suprême du Canada et le Commissariat a obtenu le statut d'intervenant.

Cette affaire a soulevé des questions qui sont des priorités stratégiques pour le Commissariat, notamment l'intégrité de l'identité et les technologies de l'information. Cette affaire abordait des éléments importants pour le Commissariat, notamment la protection de la vie privée des jeunes, les risques relatifs à la protection de la vie privée liés aux sites de réseautage social et la nécessité d'établir des normes sociales et des règles juridiques afin de s'adapter à l'ère d'Internet.

Dans les arguments écrits et oraux présentés devant la Cour le 10 mai 2012, il a été question du cadre légal que les tribunaux devraient observer quand il s'agit de prendre en considération le droit à la vie privée par rapport au principe de la publicité des débats judiciaires.

À l'unanimité, la Cour suprême a accueilli l'appel en partie, statuant que la requérante devrait être autorisée à garder l'anonymat dans le cadre de sa demande d'une ordonnance visant à divulguer l'identité du ou des utilisateurs de l'adresse IP concernée, et que les instances inférieures avaient commis une erreur en ne prenant pas en considération le préjudice objectivement discernable que subirait la requérante si sa demande d'anonymat n'était pas accordée.

La Cour suprême du Canada a conclu que le respect de la vie privée et la protection des enfants contre

la cyberintimidation justifiaient les restrictions à la liberté de la presse et au principe de l'audience publique.

Dans son évaluation, la Cour a estimé que le fait d'accorder l'anonymat à la requérante entraînerait un préjudice minimal à la liberté de la presse et au principe de l'audience publique par rapport aux effets bénéfiques liés au fait de protéger les enfants contre la cyberintimidation et la revictimisation au moment de la publication.

La Cour a également noté l'effet dévastateur de la publication sur les enfants victimes de cyberintimidation cherchant à obtenir justice.

Toutefois, la Cour a estimé qu'une fois l'identité de la requérante protégée, il n'était pas nécessaire d'accorder une ordonnance de non-publication concernant les autres renseignements non nominatifs sur le profil Facebook, puisque ces renseignements ne pouvaient dès lors plus être reliés à la requérante.

4.3 LOIS PROVINCIALES ET TERRITORIALES ESSENTIELLEMENT SIMILAIRES

Selon le paragraphe 25(1) de la LPRPDE, le Commissariat doit remettre tous les ans au Parlement un rapport sur « la mesure dans laquelle les provinces ont édicté des lois essentiellement similaires » à la *Loi*.

Aux termes de l'alinéa 26(2)*b*) de la LPRPDE, le gouverneur en conseil peut émettre une ordonnance excluant une organisation, une catégorie d'organisations, une activité ou une catégorie d'activités de l'application de la LPRPDE à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels dans une province dotée d'une loi essentiellement similaire à la LPRPDE.

Le 3 août 2002, Industrie Canada a publié le Processus de détermination du caractère « essentiellement similaire » d'une loi provinciale par le gouverneur en conseil, décrivant la politique et les critères utilisés afin de déterminer si une loi provinciale sera considérée comme « essentiellement similaire ». En vertu du processus, les lois essentiellement similaires :

- fournissent un mécanisme de protection des renseignements personnels conforme et équivalent à celui de la LPRPDE;
- intègrent les dix principes de l'annexe 1 de la LPRPDE;
- fournissent un mécanisme indépendant et efficace de surveillance et de recours ainsi que des pouvoirs d'enquête;
- restreignent la collecte, l'utilisation et la communication des renseignements personnels à des fins appropriées et légitimes.

Le 10 octobre 2012, la *Personal Health Information Act* (PHIA) de Terre-Neuve-et-Labrador a été déclarée essentiellement similaire à la LPRPDE. Ainsi, les dépositaires de renseignements personnels sur la santé soumis à la PHIA sont exclus de l'application de la Partie 1 de la LPRPDE en ce qui a trait à la collecte, à l'utilisation et à la communication des renseignements personnels sur la santé à Terre-Neuve-et-Labrador. La PHIA est entrée en vigueur le 1er avril 2011.

Cinq autres lois provinciales ont précédemment été déclarées essentiellement similaires à la LPRPDE :

- *Loi sur la protection des renseignements personnels dans le secteur privé du Québec*
- *Personal Information Protection Act* de la Colombie-Britannique
- *Personal Information Protection Act* de l'Alberta
- *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario (dépositaires de renseignements sur la santé)
- *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* du Nouveau-Brunswick (dépositaires de renseignements sur la santé).

4.4 COLLABORATION AVEC LES HOMOLOGUES PROVINCIAUX ET TERRITORIAUX

En 2012, nous avons poursuivi notre collaboration avec nos homologues provinciaux et territoriaux partout au Canada sur des enjeux communs en matière de conformité relative à la protection de la vie privée. Des réunions annuelles rassemblent les commissaires du gouvernement fédéral ainsi que des provinces et des territoires afin d'établir et d'appuyer de telles relations de travail.

À la fin de l'année 2011, le Commissariat a conclu un protocole d'entente révisé avec les commissaires à l'information et à la protection de la vie privée de la Colombie-Britannique et de l'Alberta, dans le but de renforcer la collaboration sur les questions relatives à la protection des renseignements personnels dans le secteur privé.

En signant ce protocole d'entente, les Commissariats ont renouvelé leur engagement envers le Forum sur les politiques relatives au secteur privé comme moyen de simplifier et d'appuyer notre collaboration. Ce forum sert de plateforme pour l'échange et la diffusion de l'information qui nous aide au final à soutenir les organisations en leur offrant des outils, des services et des connaissances.

En 2012, les trois commissariats ont publié trois publications communes destinées aux organisations du secteur privé :

- *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité* est un document d'orientation visant à aider les organisations du secteur privé à établir

des programmes efficaces de gestion de la protection de la vie privée.

- *L'infonuagique pour les petites et moyennes entreprises : Responsabilités et points importants touchant la protection des renseignements personnels* explique l'infonuagique et aborde des enjeux relatifs à la protection de la vie privée comme la transparence, la sécurité et le consentement.

- *Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée* offre aux concepteurs d'applications mobiles des outils afin de comprendre leurs obligations en matière de conformité aux lois relatives à la protection de la vie privée.

Nous avons également collaboré avec plusieurs de nos homologues provinciaux et territoriaux à l'élaboration d'une *Trousse d'urgence pour la protection des renseignements personnels* dans le but d'inciter les organisations à mettre en place des bonnes pratiques pour le traitement des renseignements personnels en cas d'urgence. Plusieurs organismes provinciaux et territoriaux travaillent à l'élaboration de documents connexes qui figureront, sous forme d'hyperliens, dans nos lignes directrices.

Voir les chapitres 2 et 3 du présent rapport pour plus de renseignements sur ces publications et sur d'autres documents.

4.5 INITIATIVES MONDIALES

Reconnaissant que les avancées extraordinaires réalisées dans les secteurs des technologies de l'information et des communications engendrent des défis sans précédent pour la protection des renseignements personnels, plusieurs États et organisations internationales ont commencé à s'adapter à cette nouvelle réalité. Le Commissariat continue de surveiller de nombreux aspects de ces travaux et d'y participer.

En janvier 2012, la Commission européenne a proposé une réforme complète des règles en matière de protection des données qui s'appliquent à l'ensemble de l'Union européenne. Ces réformes visent notamment à renforcer fortement les pouvoirs en matière d'application de la loi des commissaires européens à la protection des données et de la vie privée, qui seraient ainsi autorisés à imposer aux entreprises contrevenantes des amendes pouvant aller jusqu'à 1 million d'euros, ou jusqu'à 2 % de leur revenu annuel total.

Pour sa part, l'Organisation de coopération et de développement économiques (OCDE) termine l'examen de ses *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, adoptées il y a plus de 30 ans, afin de décider si elles doivent être révisées à la lumière des changements sociaux et économiques. La commissaire Stoddart a présidé un groupe d'experts

bénévoles qui a proposé plusieurs changements à apporter à ces lignes directrices.

Aux États-Unis, le président Barack Obama a rendu public le *Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, qui propose une déclaration des droits des consommateurs américains en matière de protection de la vie privée. Après un long examen, le gouvernement australien a modifié sa loi relative à la protection de la vie privée afin d'octroyer à son commissaire des pouvoirs additionnels.

Au Canada, le projet de loi visant à mettre en œuvre les améliorations à la LPRPDE qui ont été recommandées par un comité parlementaire il y a six ans n'avance pas, et le second examen obligatoire de la LPRPDE accuse un retard.

4.5.1 *Application concertée*

Par conséquent, le modèle d'application de la loi prévu dans la LPRPDE semble de plus en plus dépassé. Tandis que nous attendons que la LPRPDE soit modifiée pour inclure de nouveaux pouvoirs ou outils d'application de la loi, nous avons tenté d'être plus efficaces dans cet environnement difficile notamment en travaillant plus étroitement avec nos homologues internationaux.

En 2012, le Commissariat a conclu des ententes écrites avec les commissaires à la protection de la vie privée de l'Allemagne et du Royaume-Uni, ce qui nous a permis de partager de l'information sur les questions d'intérêt commun relatives à l'application de la loi.

Grâce à une entente similaire que nous avons signée l'année précédente avec le commissaire néerlandais, nous avons également conclu en 2012 notre toute première enquête coordonnée avec une autorité étrangère de protection des données. En tirant profit de l'expertise du commissariat néerlandais, nous avons été en mesure de mener une enquête plus complète et plus efficace sur WhatsApp, une application de messagerie mobile. L'enquête, présentée en détail dans la section 2.4 du présent rapport, a été une expérience d'apprentissage très enrichissante pour les deux commissariats.

Cette action coordonnée était une première mondiale — une enquête internationale sur les pratiques relatives à la protection de la vie privée d'une société dont l'application mobile est utilisée par de plus en plus de personnes dans le monde.

Cet effort a finalement mené à de meilleures pratiques de protection de la vie privée pour l'application WhatsApp et à une application mobile plus respectueuse de la protection de la vie privée pour des millions de Canadiennes et Canadiens et d'autres utilisateurs dans le monde. Cette expérience prouve que les autorités de protection des données peuvent collaborer pour provoquer des changements importants dans un monde de plus en plus mobile et sans frontières.

En sa qualité de coprésidente d'un groupe de travail chargé de l'élaboration d'un cadre et de

processus visant à faciliter les mesures coordonnées d'application de la loi, la commissaire a également organisé une réunion internationale afin de discuter de façons de surmonter les obstacles au partage de l'information et d'explorer des domaines propices à des efforts concertés. La réunion organisée en mai 2012 à Montréal a réuni le contrôleur européen de la protection des données et d'autres représentants du domaine de la protection des données et des organismes d'application de la loi du Canada, de la France, de l'Allemagne, de la Corée, du Mexique, des Pays-Bas, de la Nouvelle-Zélande, de la Pologne, du Royaume-Uni, de l'Uruguay et des États-Unis.

Les participants ont également convenu de dix mesures pour promouvoir une coordination efficace des mesures d'application. *Le Cadre pour la coordination internationale de l'application de la loi* a finalement été présenté à la 34e conférence internationale des commissaires à la protection des données et de la vie privée en Uruguay.

4.5.2. *Autres activités internationales*

Le Commissariat poursuit sa collaboration avec des organisations internationales dans le cadre de plusieurs autres initiatives importantes visant à protéger la vie privée. Quelques-unes des activités internationales auxquelles nous avons participé l'an dernier sont résumées ci-dessous :

- En 2012, le Consortium World Wide Web, la principale organisation internationale de normalisation pour le Web, a mis sur pied un groupe d'experts chargé de surveiller les enjeux relatifs à la protection de la vie privée liés au Web et de développer des normes afin d'y remédier. Le Commissariat préside ce nouveau **groupe d'intérêt en matière de protection de la vie privée** qui devrait dans les années à venir étudier des sujets tels que le suivi en ligne, les données relatives à la l'emplacement, à la santé et à la situation financière, les projets de cybergouvernement, le réseautage social en ligne et l'identité. Le groupe examinera également des thèmes plus vastes, comme l'empreinte du navigateur Web, qui peut être utilisé pour identifier les utilisateurs. Le groupe travaille notamment à la création d'un document-cadre sur les « considérations en matière de protection de la vie privée » afin d'aider les concepteurs de normes à intégrer les principes relatifs à la protection de la vie privée dans leurs travaux.

- Le Commissariat a participé à la conférence annuelle de l'***Association francophone des autorités de protection des données personnelles*** au cours de laquelle la commissaire adjointe a fait une présentation sur l'importance de l'expertise technique pour les autorités de protection des données en cette ère d'évolution du numérique. De concert avec les autorités de protection des données de la France, de la Suisse et du Québec, nous avons proposé avec succès que le gouvernement canadien appuie une résolution internationale qui sera intégrée à la Déclaration de Kinshasa, qui a conclu le XIVe Sommet de la francophonie. Cette

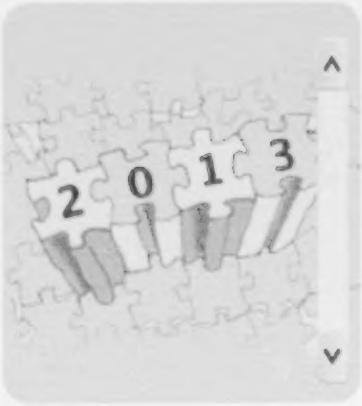
résolution reconnaît le rôle d'Internet dans la promotion des droits de la personne, de la liberté d'expression et de la participation démocratique. Elle vise également l'adoption de règles internationales contraignantes et de lois nationales définissant les principes d'une protection efficace des droits et des libertés de la personne dans le cadre du traitement des données personnelles.

- Nous avons poursuivi nos travaux avec l'**International Working Group on Data Protection in Telecommunications**, mieux connu sous le nom de « groupe de Berlin ». Créée en 1983, cette organisation a pour but de sonner l'alerte rapidement quant aux risques émanant des nouveaux développements technologiques. Au cours des dernières années, l'organisation s'est penchée sur un éventail de sujets, comme les renseignements de localisation mobile, le vote en ligne, la surveillance des télécommunications, l'infonuagique, les compteurs intelligents, les micropaiements électroniques et les enregistreurs de données routières du véhicule. Les résultats des délibérations du groupe de travail sont accessibles en ligne en allemand et en anglais.

- Un membre de notre équipe représente le Canada dans un groupe de travail de l'**Organisation internationale de normalisation** (ISO) qui traite de la gestion de l'identité et des technologies de protection de la vie privée. Le groupe de travail a déjà publié une série de normes internationales visant à renforcer la sécurité des données personnelles dans diverses pratiques nécessitant des technologies d'authentification, dont la biométrie. Le groupe se penche également sur d'autres sujets, notamment la protection des données dans l'infonuagique, la confirmation de l'identité, la méthode d'évaluation des facteurs relatifs à la vie privée, la suppression sécurisée des données et les réseaux intelligents.

L'année à venir

Comme le démontre le présent rapport, 2012 a été une année chargée pour le Commissariat. Et nous avons toutes les raisons de penser que l'année 2013 sera tout aussi occupée, et probablement même plus encore.



Nous ne pouvons pas par exemple espérer que les menaces actuelles pour la protection de la vie privée disparaissent miraculeusement. Les défis engendrés par la technologie devraient vraisemblablement continuer de prendre de l'expansion.

En outre, le Commissariat va traverser la rivière des Outaouais pour s'établir à Gatineau (Québec), à l'automne, avec le tumulte et la perturbation que représente un déménagement. Nous serons rejoints dans ce nouvel édifice par d'autres agents du Parlement — le Commissariat aux langues officielles, Élections Canada et le Commissariat à l'information du Canada. Dans un souci de plus grande efficacité, nous partagerons une bibliothèque, une salle de traitement du courrier, une salle de serveurs et un centre de données.

De plus, les dix années de la commissaire Stoddart à la tête de notre organisation arriveront à leur terme en décembre, amorçant une période de préparation et de transition vers un nouveau leadership.

De notre point de vue, toute cette activité n'est pas négative. Au contraire, elle rend une organisation comme la nôtre dynamique et pleine de vivacité. Cette situation nous force à examiner de manière critique ce que nous faisons, à veiller à ce que nos activités soient sensibles, pertinentes et rationalisées.

Notre but n'est pas simplement de faire notre travail; nous voulons avoir une incidence sur la vie des Canadiennes et Canadiens — une incidence importante et positive.

C'est ce qui nous donne de l'énergie. En d'autres termes, c'est une bonne chose d'avoir un calendrier bien rempli.

Dans ce contexte, voici ce que nous avons prévu pour 2013 :

Réforme législative

L'environnement dans lequel les renseignements personnels sont recueillis, utilisés et communiqués a connu une transformation radicale depuis l'adoption

de la LPRPDE. L'incroyable capacité des ordinateurs modernes à collecter, conserver, manipuler et interpréter les données a fait des renseignements personnels une marchandise en demande.

Les nouvelles technologies ont permis de créer de nouveaux produits et services attrayants pour les consommateurs. Mais, elles s'accompagnent également de risques, notamment la perte, le vol ou le détournement des renseignements personnels.

En dépit de tous les efforts mis en œuvre par le Commissariat pour inciter les organisations à signaler les atteintes à la protection des données, nous ne connaissons toujours pas l'étendue de telles fuites. En effet, tandis que le Parlement continue de se pencher sur un projet de loi visant à rendre obligatoire le signalement des atteintes, force est d'admettre que les entreprises qui ne signalent pas ces incidents bénéficient d'un avantage concurrentiel par rapport aux entreprises responsables qui les signalent.

Nous avons également connu quelques difficultés dans nos efforts pour veiller à ce que les organisations qui ont fait l'objet d'une enquête mettent effectivement en œuvre les changements promis. Au cours des enquêtes, nous avons fréquemment remarqué que les mesures de protection de la vie privée n'ont pas été intégrées aux produits et services. Nous avons ensuite rencontré des problèmes pratiques pour veiller à ce que les organisations assument la responsabilité des mesures de suivi qu'elles ont acceptées de mettre en œuvre à la fin de l'enquête.

Il faut généralement plus de temps que le délai prévu en vertu de la loi pour passer devant la Cour fédérale et faire appliquer les recommandations de la commissaire. Dans ce contexte, il est difficile de veiller à ce que les changements pertinents soient apportés pour remédier aux problèmes.

En raison d'une autre lacune de la loi actuelle, nous sommes incapables de déterminer à quelle fréquence les organisations sont contraintes de divulguer les renseignements personnels de leurs clients à la demande de la police ou d'autres agents d'application de la loi. La divulgation de ces renseignements peut avoir des ramifications importantes pour les personnes, mais le voile sur ces divulgations est opaque et absolu.

La LPRPDE est une loi fondée sur des principes, ce qui lui procure force et souplesse. Cependant, nous avons conclu que des mesures incitatives sont nécessaires pour veiller à ce que les organisations intègrent des mesures de protection de la vie privée dans leurs produits et services dès le départ.

C'est la raison pour laquelle nous sommes en faveur d'un renforcement des pouvoirs d'application de la loi, comme le pouvoir de prendre des ordonnances et d'imposer des sanctions financières en cas d'infractions à la *Loi*. Nous sommes également favorables à une obligation de signalement des atteintes, à un rapport public des divulgations à l'insu de la personne ou sans son consentement en vertu de la disposition d'« autorité légitime » et à un renforcement des obligations de responsabilité pour les organisations.

En 2013, nous continuerons de faire pression pour amener les changements nécessaires à la LPRPDE

et aux autres lois, afin de veiller à ce que les renseignements personnels des Canadiennes et Canadiens soient protégés et que leur confiance soit assurée dans cette économie numérique complexe et en pleine expansion.

Nous sommes préoccupés par le projet de loi C-12, la *Loi protégeant les renseignements personnels des Canadiens*, qui modifierait la LPRPDE pour introduire les obligations de signalement des atteintes et élargir les raisons pour lesquelles les organismes d'application de la loi pourraient obtenir des renseignements personnels de la part des organisations. Au moment de la rédaction du présent rapport, le projet de loi, présenté à la Chambre des communes en septembre 2011, n'avait pas encore été débattu.

Plaintes et enquêtes

Le traitement des demandes d'information et des plaintes des particuliers relativement à la protection de leur vie privée reste au cœur de nos activités principales et nous continuerons de chercher des façons de maximiser notre influence à cet égard.

Nous continuerons à améliorer et à simplifier nos processus afin de réduire le temps nécessaire au traitement des plaintes. Nous mettrons davantage l'accent sur l'intervention de première ligne, grâce à une participation plus active de notre Centre d'information et de notre unité de réception des plaintes, ainsi qu'au moyen d'un effort concerté pour résoudre les problèmes par l'entremise de notre processus de règlement rapide.

Nous mettrons également à l'essai un nouveau processus de médiation qui visera à amener les parties à conclure un accord rapide et à s'engager à le respecter. Nous continuerons de concentrer nos ressources d'enquête sur les domaines posant les risques les plus élevés pour la protection de la vie privée des Canadiennes et Canadiens, en particulier lorsque nous choisissons d'entamer des plaintes du chef de la commissaire.

Et nous continuerons à promouvoir la conformité volontaire, en encourageant les organisations à répondre aux plaintes avant que nous ne produisions notre rapport final.

Un processus de traitement des plaintes plus opportun et plus efficace sera bénéfique tant pour les plaignants que pour les organisations mises en cause. Et cette évolution sera également positive pour l'ensemble de la population canadienne, car chaque affaire résolue contribue à renforcer la protection de la vie privée pour tous.

Loi canadienne anti-pourriel (LCAP)

La Direction des enquêtes liées à la LPRPDE continue de se préparer en vue de la charge accrue de plaintes que nous attendons du fait de l'adoption de la *Loi canadienne anti-pourriel* (LCAP), qui a reçu la sanction royale le 15 décembre 2010. Au moment de la publication du présent rapport, le règlement d'application de la LCAP n'était pas encore au point et la date d'entrée en vigueur de la n'avait pas encore été établie.

Dans l'intervalle, nous travaillons avec nos organismes partenaires — le Conseil de la

radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau de la concurrence — avec lesquels nous partageons les responsabilités d'enquête en vertu de la nouvelle loi.

Et nous renforçons notre capacité technologique, de sorte que nos enquêteurs seront correctement formés pour examiner les plaintes de collecte non autorisée de renseignements personnels au moyen d'espiogiciels ou de la collecte d'adresses électroniques.

Recherche et orientation stratégique

Au cours de l'année à venir, le Commissariat poursuivra son approche proactive visant à identifier et à explorer les nouveaux enjeux en matière de protection de la vie privée. Nos efforts internes de recherche renforcent l'expertise de notre effectif et appuient l'orientation que nous offrons aux entreprises et à d'autres intervenants.

Nous songeons déjà à plusieurs sujets importants, notamment les paiements mobiles, les logiciels de reconnaissance faciale et les meilleures façons d'obtenir le consentement pour la collecte des renseignements personnels dans un environnement en ligne.

Un autre sujet particulièrement difficile que nous allons examiner attentivement est celui des sites Web de « vengeance », qui permettent aux personnes de publier des informations et des photos insultantes et humiliantes à propos d'autres personnes, souvent un ex-conjoint ou un ex-partenaire amoureux. Lorsque les sites Web de vengeance refusent les demandes des personnes ciblées de retirer les photos et les commentaires, ces personnes se tournent vers nous pour obtenir la protection de leur vie privée en vertu de la loi. Au cours de l'année à venir, le Commissariat élaborera et diffusera un document de recherche qui étudiera cette problématique et ses répercussions sur la protection de la vie privée.

Collaboration avec d'autres autorités de protection des données

Comme nous le faisons depuis quelques années déjà, nous continuerons à collaborer avec nos homologues provinciaux et territoriaux sur des enquêtes conjointes et l'élaboration de lignes directrices.

De même, nous continuerons d'établir des relations efficaces avec nos homologues internationaux afin d'enquêter sur des enjeux d'intérêt commun ou d'y remédier. Nous sommes persuadés qu'il s'agit de la meilleure manière de renforcer la protection des renseignements personnels dans un monde interconnecté.

Soulignons en outre que 2013 sera marquée par le premier ratissage mondial d'Internet du Global Privacy Enforcement Network (GPEN). Initiative chapeautée par le Commissariat, le ratissage réunit des autorités chargées de l'application des lois sur la protection de la vie privée du monde entier dans un effort coordonné visant à identifier les enjeux et les tendances potentiels relatifs à la protection de la vie privée dans le secteur commercial. Ainsi, pour la première année de cette initiative, plus d'une douzaine d'autorités de protection de la vie privée internationales et canadiennes braquent les projecteurs sur la transparence des pratiques des organisations en matière de confidentialité. Cette année, le Commissariat assumera un rôle de coordination.

Annexe 1

Définitions

DÉFINITIONS DES TYPES DE PLAINTES DÉPOSÉES EN VERTU DE LA LPRPDE

Les plaintes adressées au Commissariat sont réparties selon les principes et les dispositions de la LPRPDE qui auraient été enfreints :

Accès : Une personne s'est vu refuser l'accès aux renseignements personnels qu'une organisation détient à son sujet ou n'a pas reçu tous les renseignements, soit en raison de l'absence de certains documents ou renseignements, soit en raison d'une exception dont l'organisation s'est prévalue pour retrancher les renseignements.

Collecte : Une organisation a recueilli des renseignements personnels non nécessaires ou les a recueillis par des moyens injustes ou illégaux.

Consentement : Une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement explicite de la personne concernée ou elle a exigé que la personne consente à la collecte, à l'utilisation ou à la communication déraisonnable de renseignements personnels comme condition à l'obtention des biens ou des services.

Conservation : Les renseignements personnels sont conservés plus longtemps qu'il n'est nécessaire aux fins qu'une organisation a déclarées au moment de la collecte des renseignements ou, s'ils ont été utilisés pour prendre une décision au sujet d'une personne, l'organisation n'a pas conservé les renseignements assez longtemps pour permettre à la personne d'y avoir accès.

Correction/Annotation : L'organisation n'a pas corrigé, à la demande d'une personne, les renseignements personnels qu'elle détient à son sujet ou, en cas de désaccord avec les corrections demandées, n'a pas annoté les renseignements afin d'indiquer la teneur du désaccord.

Délais : Une organisation a omis de fournir à une personne l'accès aux renseignements personnels qui la concernent dans les délais prévus par la *Loi*.

Exactitude : Une organisation a omis de s'assurer que les renseignements personnels qu'elle utilise sont exacts, complets et à jour.

Frais : Une organisation a exigé plus que des frais minimaux pour fournir à des personnes l'accès à leurs renseignements personnels.

Mesures de sécurité. Une organisation n'a pas protégé les renseignements personnels qu'elle détient par des mesures de sécurité appropriées.

Possibilité de porter plainte : Une organisation a omis de mettre en place les procédures ou les politiques qui permettent à une personne de porter plainte en vertu de la *Loi* ou elle a enfreint ses propres procédures et politiques.

Responsabilité : Une organisation a failli à l'exercice de ses responsabilités à l'égard des renseignements personnels qu'elle possède ou dont elle a la garde ou elle a omis de désigner une personne responsable de surveiller le respect de la *Loi*.

Transparence : Une organisation a omis de rendre facilement accessibles aux personnes des renseignements précis sur ses pratiques et politiques en matière de gestion des renseignements personnels.

Utilisation et communication : Les renseignements personnels sont utilisés ou communiqués à des fins autres que celles pour lesquelles ils avaient été recueillis, sans le consentement de la personne concernée, et l'utilisation ou la communication de renseignements personnels sans le consentement de la personne concernée ne font pas partie des exceptions prévues dans la *Loi*.

DÉFINITIONS DES CONCLUSIONS ET AUTRES DÉCISIONS

Au début de l'année 2012, le Commissariat a modifié certaines des définitions des conclusions et des décisions afin qu'elles expriment mieux les résultats de nos enquêtes en vertu de la LPRPDE. Ces nouvelles décisions avaient également pour but de mieux refléter les responsabilités des organisations à rendre des comptes en vertu de la *Loi*.

Les définitions ci-dessous expliquent ce que signifie chaque décision.

Non fondée : L'enquête n'a pas permis de déceler des éléments de preuve donnant à penser qu'une organisation a enfreint la LPRPDE ou de déceler assez d'éléments de preuve à cette fin.

Fondée et conditionnellement résolue : La commissaire a déterminé qu'une organisation avait enfreint une disposition de la LPRPDE. L'organisation s'est engagée à mettre en œuvre les recommandations formulées par la commissaire et à faire la démonstration de cette mise en œuvre dans les délais prescrits.

Fondée et résolue : La commissaire a déterminé qu'une organisation avait enfreint une disposition de la LPRPDE. L'organisation a démontré qu'elle avait pris des mesures correctives satisfaisantes pour remédier à la situation, soit de sa propre initiative, soit à la suite de recommandations formulées par la commissaire, au moment où la conclusion a été rendue.

Fondée : La commissaire a déterminé qu'une organisation avait enfreint une disposition de la LPRPDE.

Réglée rapidement : Le Commissariat a aidé à négocier une solution satisfaisante pour toutes les parties concernées sans qu'une enquête officielle n'ait été entreprise. La commissaire ne produit pas de rapport.

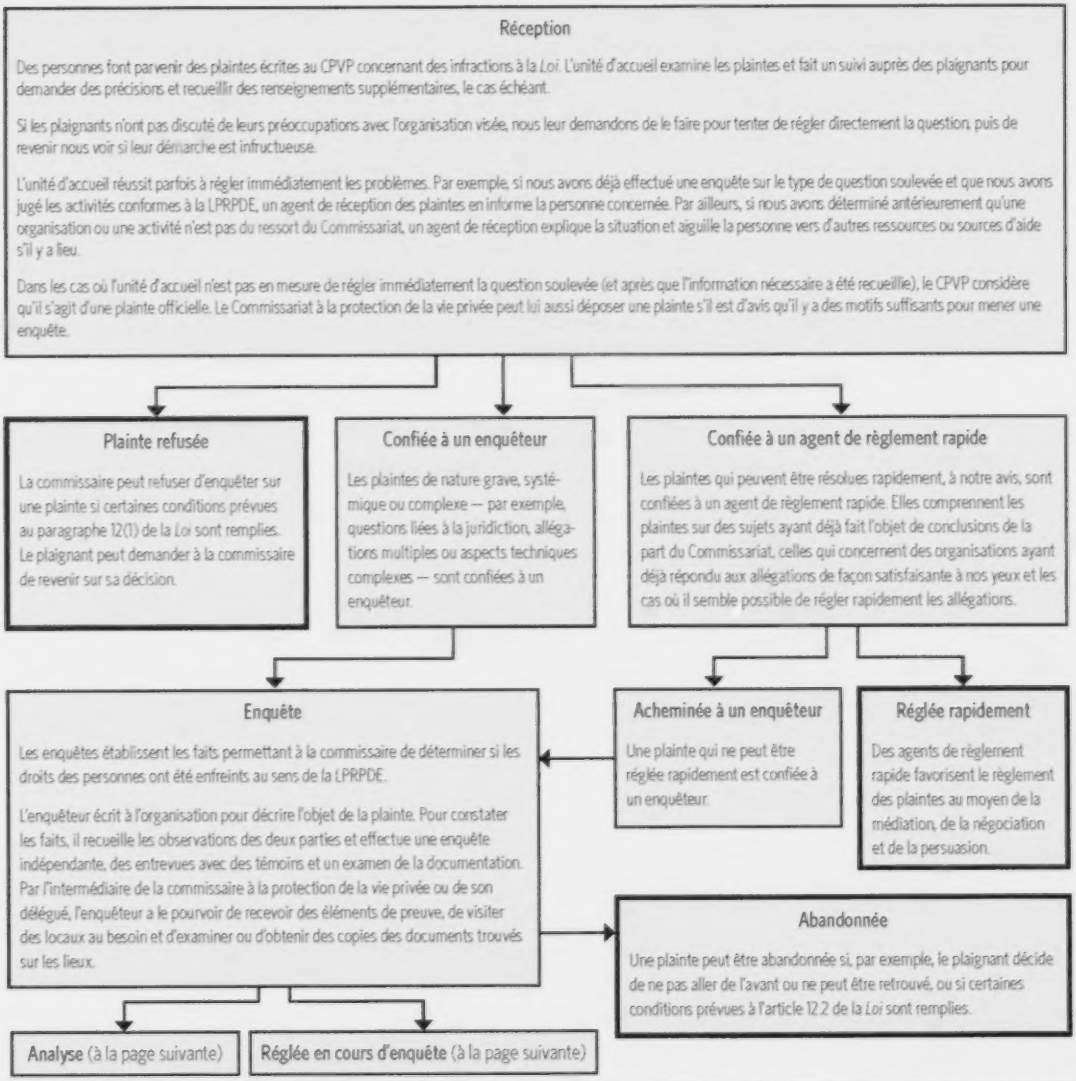
Réglée en cours d'enquête : Le Commissariat aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. La commissaire ne produit pas de rapport.

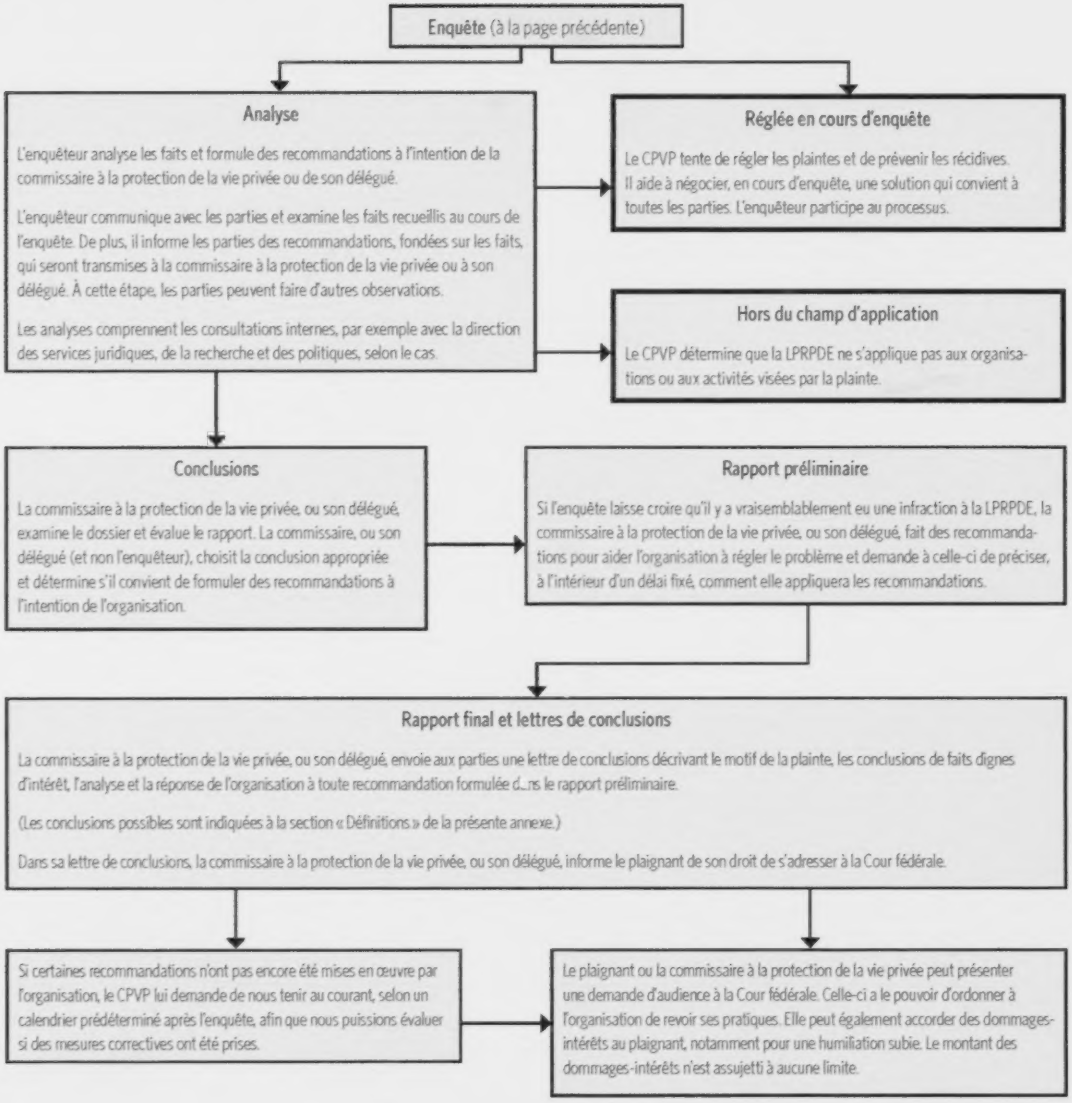
Mettre fin à l'examen : L'enquête a pris fin avant que toutes les allégations ne soient pleinement examinées. À sa discrétion, la commissaire peut mettre fin à l'examen de la plainte pour un motif prévu au paragraphe 12.2(1) de la LPRPDE, à la demande du plaignant ou lorsqu'il a renoncé à la plainte.

Refus d'enquêter : La commissaire a refusé de procéder à une enquête relative à une plainte parce qu'elle était d'avis que le plaignant aurait d'abord dû épuiser les recours internes ou les procédures d'appel ou de règlement des griefs qui lui sont normalement ouverts; que la plainte pourrait avantageusement être instruite selon des procédures prévues par le droit fédéral ou le droit provincial; que la plainte n'a pas été déposée dans un délai raisonnable après que son objet a pris naissance, conformément au paragraphe 12(1) de la LPRPDE.

Hors du champ d'application : À la lumière des données préliminaires recueillies, on a déterminé que la LPRPDE ne s'appliquait pas à l'organisation ou à l'activité faisant l'objet de la plainte. La commissaire ne produit pas de rapport.

PROCESSUS D'ENQUÊTE




Enquête (à la page précédente)
Analyse
L'enquêteur analyse les faits et formule des recommandations à l'intention de la commissaire à la protection de la vie privée ou de son délégué.
L'enquêteur communique avec les parties et examine les faits recueillis au cours de l'enquête. De plus, il informe les parties des recommandations, fondées sur les faits, qui seront transmises à la commissaire à la protection de la vie privée ou à son délégué. À cette étape, les parties peuvent faire d'autres observations.
Les analyses comprennent les consultations internes, par exemple avec la direction des services juridiques, de la recherche et des politiques, selon le cas.
Réglée en cours d'enquête
Le CPVP tente de régler les plaintes et de prévenir les récidives. Il aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. L'enquêteur participe au processus.
Hors du champ d'application
Le CPVP détermine que la LPRPDE ne s'applique pas aux organisations ou aux activités visées par la plainte.
Conclusions
La commissaire à la protection de la vie privée, ou son délégué, examine le dossier et évalue le rapport. La commissaire, ou son délégué (et non l'enquêteur), choisit la conclusion appropriée et détermine s'il convient de formuler des recommandations à l'intention de l'organisation.
Rapport préliminaire
Si l'enquête laisse croire qu'il y a vraisemblablement eu une infraction à la LPRPDE, la commissaire à la protection de la vie privée, ou son délégué, fait des recommandations pour aider l'organisation à régler le problème et demande à celle-ci de préciser, à l'intérieur d'un délai fixé, comment elle appliquera les recommandations.
Rapport final et lettres de conclusions
La commissaire à la protection de la vie privée, ou son délégué, envoie aux parties une lettre de conclusions décrivant le motif de la plainte, les conclusions de faits dignes d'intérêt, l'analyse et la réponse de l'organisation à toute recommandation formulée d...ns le rapport préliminaire.
(Les conclusions possibles sont indiquées à la section « Définitions » de la présente annexe.)
Dans sa lettre de conclusions, la commissaire à la protection de la vie privée, ou son délégué, informe le plaignant de son droit de s'adresser à la Cour fédérale.
Si certaines recommandations n'ont pas encore été mises en œuvre par l'organisation, le CPVP lui demande de nous tenir au courant, selon un calendrier prédéterminé après l'enquête, afin que nous puissions évaluer si des mesures correctives ont été prises.
Le plaignant ou la commissaire à la protection de la vie privée peut présenter une demande d'audience à la Cour fédérale. Celle-ci a le pouvoir d'ordonner à l'organisation de revoir ses pratiques. Elle peut également accorder des dommages-intérêts au plaignant, notamment pour une humiliation subie. Le montant des dommages-intérêts n'est assujetti à aucune limite.

Annexe 2

Statistiques sur les enquêtes liées à la LPRPDE pour 2012

PLAINTES ACCEPTÉES, PAR SECTEUR D'ACTIVITÉ*

Secteur	Nombre	Proportion de toutes les plaintes acceptées
Secteur financier	49	22 %
Services	22	10 %
Internet	23	10 %
Assurance	15	7 %
Ventes/Détail	16	7 %
Services professionnels	6	3 %
Transports	11	5 %
Télécommunications	23	10 %
Hébergement	19	9 %
Santé	6	3 %
Divertissement	7	3 %
Autres	23	10 %
Total	**220**	**100 %**

* Les secteurs d'activité sont définis ci-dessous.

DÉFINITIONS DES SECTEURS D'ACTIVITÉ :

- **Secteur financier :** banques, intermédiation financière (p. ex. société émettrice de cartes de crédit, financement des ventes, prêts à la consommation, courtiers hypothécaires, activités de traitement des transactions financières), investissement financier et activités connexes, planification et investissement financiers, autorités monétaires.

- **Services :** organisations civiques et professionnelles, services de soins personnels, services de réparation et de maintenance, programmes de récompense, services administratifs et de soutien (comprend les agences de recouvrement et les agences d'évaluation du crédit), services éducatifs et aide sociale.

- **Internet :** traitement des données, hébergement Web et services connexes, fournisseurs de services Internet, réseaux sociaux et portails de recherche Web.

- **Assurance :** sociétés d'assurance (responsabilité, vie, maladie, dommages et décès).

- **Vente/Détail :** concessionnaires d'automobiles, vente de matériaux de construction et de fournitures, marketing direct, commerce électronique, vente au détail (en magasin et en ligne).

- **Services professionnels :** comptabilité, préparation de déclarations de revenus tenue de comptes et services de la paie, services juridiques, autres services professionnels, scientifiques et techniques.

- **Transports :** transport par voie aérienne et ferroviaire, transport en commun et transport terrestre de voyageurs, camionnage, transport par voie d'eau.

- **Télécommunications :** applications mobiles, entreprises de télécommunications par satellite, équipement de télécommunications, entreprises de télécommunications câblées ou sans fil.

- **Hébergement :** associations de condominiums, coopératives d'habitation, services immobiliers, logements locatifs et hébergement des voyageurs.

- **Santé :** médecins, dentistes, pharmaciens et autres professionnels de la santé.

- **Divertissement :** industries du divertissement, du jeu et des loisirs et autres services de divertissement.

PLAINTES ACCEPTÉES, PAR TYPE DE PLAINTE

Type de plainte	Nombre	Proportion de toutes les plaintes acceptées
Accès	65	30 %
Responsabilité	7	3 %
Exactitude	6	3 %
Fins appropriées	2	1 %
Possibilité de porter plainte	1	1 %
Collecte	33	15 %
Consentement	14	6 %
Correction/Annotation	10	5 %
Frais	1	1 %
Détermination des fins de la collecte	1	1 %
Transparence	1	1 %
Conservation	6	3 %
Mesures de sécurité	17	8 %
Utilisation et communication	56	26 %
TOTAL	220	100 %*

* Les totaux peuvent ne pas égaler 100 % en raison de l'arrondissement.

PLAINTES FERMÉES, PAR SECTEUR D'ACTIVITÉ ET DÉCISION

Secteur	Réglée rapidement	Décisions relatives aux affaires ayant fait l'objet d'une enquête										Sous-total de toutes les affaires ayant fait l'objet d'une enquête	Total des résolutions rapides et des enquêtes
		Non fondée	Hors juridiction	Abandonnée	Fondée et conditionnellement résolue	Fondée et résolue	Fondée	Résolue	Réglée en cours d'enquête	Retrait	Refus d'enquêter		
Secteur financier	18	9		3		12	3		3	4		34	**52**
Services	10	5				4			9			18	**28**
Internet	8	2	1	1	7	3	1	1	4			20	**28**
Assurance	10	4	1	2	1	4	1		1	6		20	**30**
Ventes/Détail	13		1	1		3				1		6	**19**
Services professionnels	3									1	1	2	**5**
Transports	10	2		2		5			2			11	**21**
Télécommunications	11	1		2		9				2		14	**25**
Hébergement	16	2	1	2		1			1	1		8	**24**
Santé	0		1		1							2	**2**
Divertissement	3				2	2						4	**7**
Autres	13		1	1					2	2		6	**19**
Total	115	25	6	14	11	43	5	1	22	17	1	145	**260**

PLAINTES FERMÉES, PAR TYPE DE PLAINTE ET DÉCISION

	Décision rendue										
Type de plainte	Non fondée	Hors du champ d'application	Abandonnée	Fondée et conditionnellement résolue	Fondée et résolue	Fondée	Résolue	Réglée en cours d'enquête	Retrait	Refus d'enquêter	Total
Utilisation et communication	8	4	5	3	12	4	1	6	4	1	48
Accès	3	1	4		13			2	5		28
Collecte	7		2	1	4			3	3		20
Consentement	3	1		2	6			5	1		18
Correction/Annotation	3				2			3	1		9
Conservation	1		1	1		1		1			5
Mesures de sécurité			1		2			1	1		5
Responsabilité					2			1			3
Exactitude									2		2
Possibilité de porter plainte					1						1
Frais					1						1
Transparence				2							2
Détermination des fins de la collecte				1							1
Fins appropriées			1	1							2
Total	25	6	14	11	43	5	1	22	17	1	145

DÉLAI DE TRAITEMENT MOYEN, PAR DÉCISION

Décision	Nombre	Délai de traitement moyen (en mois)
Réglée rapidement	115	2,8
Abandonnée	14	8,5
Hors du champ d'application	6	9,0
Non fondée	25	14,3
Résolue	1	1,0
Réglée en cours d'enquête	22	10,2
Fondée	5	17,5
Fondée et conditionnellement résolue	13	16,4
Fondée et résolue	41	16,1
Retrait	17	5,9
Refus d'enquêter	1	9,0
Total	**260**	—
Moyenne pondérée globale	—	**8,3**

DÉLAI DE TRAITEMENT MOYEN, PAR TYPE DE PLAINTE ET DE RÈGLEMENT

Type de plainte	Règlement rapide		Plaintes officielles	
	Nombre	Délai de traitement moyen (en mois)	Nombre	Délai de traitement moyen (en mois)
Accès	38	2,8	29	10,9
Responsabilité	3	2,5	3	10,6
Exactitude			2	8
Fins appropriées			2	19
Possibilité de porter plainte	1	2,8	1	12
Collecte	25	2,7	20	11,8
Consentement	1	1,2	18	14,6
Correction/Annotation	5	3,2	9	12
Frais			1	16
Détermination des fins de la collecte			1	25
Transparence			2	25,5
Conservation	5	5,8	5	19,4
Mesures de sécurité	8	1,8	5	19,4
Utilisation et communication	29	2,8	47	12
Total	**115**	—	**145**	—
Moyenne pondérée globale en mois	—	**2,8**	—	**12,6**

SIGNALEMENTS VOLONTAIRES DES ATTEINTES À LA PROTECTION DES DONNÉES, PAR SECTEUR D'ACTIVITÉ ET TYPE D'INCIDENT

Secteur d'activité	Type d'incident*			Total des incidents par secteur	Proportion de tous les incidents
	Communication accidentelle	Perte	Accès, utilisation ou communication non autorisés		
Secteur financier	4	2	13	19	58 %
Services			1	1	3 %
Assurance	2			2	6 %
Ventes/Détail					
Télécommunications			3	3	9 %
Internet			1	1	3 %
Divertissement	1		2	3	9 %
Hébergement	1		1	2	6 %
Autre		1		1	3 %
Santé					
Services professionnels	1			1	3 %
Transports					
Total	**9**	**3**	**21**	**33**	100 %

* Voir les définitions ci-dessous.

Définitions des types d'atteinte à la protection des données

Communication accidentelle : incidents dans le cadre desquels une organisation communique par accident des renseignements personnels à des personnes auxquelles ces renseignements ne sont pas destinés, par exemple, des relevés bancaires envoyés à la mauvaise adresse en raison d'une erreur mécanique ou humaine, ou des renseignements personnels rendus publics sur le site Web d'une organisation à la suite d'une erreur technique

Perte : incidents dans le cadre desquels des renseignements personnels sont perdus par une organisation, habituellement à la suite de la perte d'un ordinateur portatif, d'un CD ou de documents papier

Accès, utilisation ou communication non autorisés : incidents dans le cadre desquels une personne utilise ou communique des renseignements personnels ou y accède sans l'autorisation d'une organisation, par exemple, à la suite du vol d'un ordinateur portatif, du piratage en ligne de la base de données d'une organisation ou de l'utilisation de renseignements personnels, ou de l'accès à ceux-ci, par un employé à des fins non autorisées.